Doktori (PhD) értekezés

Holló Krisztina
2022.

NEMZETI KÖZSZOLGÁLATI EGYETEM

Közigazgatás-tudományi Doktori Iskola

Holló Krisztina

A biztonságtudatosság hiánya, mint kockázati tényező vizsgálata
különös tekintettel az adatvédelmi és információbiztonsági szabályok alkalmazására

Doktori (PhD) értekezés

Témavezetők:

Dr. Leitold Ferenc

főiskolai tanár

…….

Dr. Péterfalvi Attila

egyetemi docens

……..

Budapest, 2022.

TARTALOMJEGYZÉK

1. BEVEZETÉS

> „Vannak a népek történetében korszakok, amelyekben az eszmék és intézmények, amelyek részt vesznek az általános fejlődésben, maguk is külön átalakuláson mennek át. Akár akarjuk, akár nem, minden jel arra vall, hogy azok az alapfogalmak, amelyek a múltban jogintézményeink alapjai voltak, szétesnek és helyüket másoknak adják át, hogy a jogrendszer, amelyen modern társadalmunk élete eddig nyugodott, feloszlik és új rendszer épül fel teljesen új eszmék alapján. Ez minden országban így van, amely a fejlődésnek ugyanarra a fokára jutott."
>
> Duguit: Les transformations du droit public, 1925

Az emberiség az információs társadalom küszöbén jelentős fejlődést hajtott végre. A több ezeréves társadalmi történelem ideje során sokáig nem tulajdonítottak jelentőséget a mai értelembe vett információnak. A régmúlt idők társadalmai, sőt a filozófia nagy mesterei közül talán senki sem gondolt az információ mai korban betöltött jelentőségére, főként nem az információrobbanásra, az információs társadalomra és az információs paradigmaváltásra. Napjainkban, az információs társadalomban a rendelkezésre álló információs rendszerek és szolgáltatások létfontosságú szerepet játszanak mind a háztartásokban, mind az üzleti életben, ezért megbízhatóságuk és biztonságuk szintje lényeges szempont. A biztonsági események nagyságrendje, gyakorisága és hatása évről évre – mondhatjuk – exponenciális mértékben növekszik, ami súlyos fenyegetést jelent az információs társadalom működésére és fenntarthatóságára. Az információs rendszerek a működésük akadályozására, károkozására vagy adatainak felhasználásával jogtalan haszonszerzésre irányuló szándékos és ártalmas cselekmények célpontjaivá válhatnak.[1] Az információs rendszereket ért incidensek nehezíthetik a mindennapos életet, a gazdasági tevékenységek gyakorlását, jelentős pénzügyi veszteségeket, valamint bizalomvesztést és súlyos károkat okozhatnak az európai közösségnek és a gazdasági tevékenységeknek. Az értekezés célja a biztonságtudatossági hiány hatásának vizsgálata, továbbá a kockázati tényezők értékelése elsődlegesen az adatvédelmi és információbiztonsági területre vonatkozóan, az információbiztonsági tudatosság hazai hiányának kezelésére fókuszálva. Az értekezés címének behatárolását és témájának dogmatikai szűkítését szolgálja az adatvédelmi és információbiztonsági szabályozási kérdések korrelációjának hangsúlyozása.

[1] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148, letöltés: 2019. június 1.

Az értekezés hátterében végzett kutatásom alapvetően a közigazgatás-tudomány területére fókuszál, szükségszerűen érinti az informatikai és a jogtudomány azon területeit, amelyek az eredmények szempontjából relevánsak, ugyanakkor a közigazgatás tudományterületeken elért eredményként terjesztem elő. A választott kutatási terület komplex és több tudományterületet érintő sajátossága tekintetében további behatárolás és pontosítás szükséges. Az értekezés súlypontját meghatározva hangsúlyozom, hogy a biztonságtudatosság hiányára vonatkozó vizsgálatokat elsődlegesen az információbiztonsági tudatosság hiányára, valamint kiterjesztve az adatvédelmi[2] [3] és információbiztonsági alapelvek és szabályok[4] összefüggéseire, alkalmazására, tudatosítására és információbiztonság-tudatosságnövelési program[5] alapján tudatosítási szintek vizsgálatára, a hiány okozataként megvalósuló incidensek tényezőire, ezek információbiztonsági kockázatkezelésére és információbiztonsági tudatosság összefüggéseire, valamint vonatkozó intézkedési típusok hatékonyságára összpontosítottam. Az értekezés eredményeinek megállapításaihoz szükséges eszközök és igazolások tekintetében fókuszba kerültek az adatvédelmi és információbiztonsági incidensek gazdasági aspektusai, az információbiztonsági kockázatkezelésnél alkalmazott módszerek, az információs társadalom sajátosságai és az európai digitális kultúra fejleszthetőségének módjai, ugyanakkor ezen témák volumenüket tekintve kizárólag a kutatás igazolásának forrásai vagy eszközei, a háttérkutatás részét képezik.

Összegezve az értekezés a hazai információbiztonsági tudatosság helyzetére, a hiányának sajátosságaira, azok következményeire és pótlásának lehetőségeire keresi a választ, különösen a releváns folyamatok mely tényezőiről és eredményeiről beszélhetünk az adatvédelmi és információbiztonsági, valamint az információbiztonsági tudatosítási folyamatok és kapcsolatok tekintetében. Az említett folyamatokhoz igazodva, az értekezés szerkezetét tekintve az európai és hazai adatvédelmi és az információbiztonsági történeti és szabályozásának vonulatából, valamint a biztonságtudatosság, különös tekintettel az információbiztonság és az információbiztonsági tudatosság helyzetéből kiindulva, szűkítő jelleggel jut el az adatvédelmi és információbiztonsági jogalkotás és a digitális kultúra fejlesztésének igényéig.

---

[2] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
[3] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)
[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (IBtv.)
[5] Mádi-Nátor Anett, Kardos Zoltán, Nemzeti Közszolgálati Egyetem, Mádi-Nátor Anett, Kardos Zoltán, Információbiztonság-tudatosság gyakorlat, Nemzeti Közszolgálati Egyetem, https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsag-tudatossag-gyakorlat.original.pdf, letöltés: 2022. január 18.

1.1. A KUTATÁS HÁTTERE ÉS AKTUALITÁSA

A múlt század elején még semmi jel nem mutatott arra, hogy az évszázad végére egy teljesen új társadalmi rendszer fog kialakulni. A hírközléstechnika megjelenésével és rohamos fejlődésével egy olyan technikai és kulturális forradalmi változás ment végbe, ami egészen egyedi és példaértékű. Az információs társadalom fogalma a huszadik század elején még teljesen ismeretlen volt. Az információelmélet megalkotásával 1948-ban egy új korszak született az információvédelem terén. Az információelmélet, az információkutatás és -tudomány[6] első, kezdeti szakasza az információ olyan jelentőségét ismerte fel, amit még korábban egyáltalán nem. Claude Elwood Shannon: A Mathematical Theory of Communication (The Bell System Technical Journal), és Norbert Wiener „*Cybernetics or Control and Communication in the Animal and the Machine*" című műve 1948-ban történelmet írt, meghatározva az információ jelentőségét a mai kor számára is. A tudás és az információ szerepe mindig meghatározó volt a gazdaság és a társadalom életében, így napjainkban a felgyorsult társadalmi, gazdasági, technológiai fejlődés folyamatai ezt a szerepet folyamatosan alakítják. Az utóbbi évszázadban fontossá vált a gyors, biztonságos elektronikus információáramlás[7] és a támogató folyamatok, technológiák mindenkori rendelkezésre állása, az egyéni tudás megszerzése, terjesztése, fejlesztése, mind a versenyszférában, mind a közigazgatásban egyaránt. A matematikus Norbert Wiener alapvető tézise, hogy a szabályozás, úgymint az információ is egy olyan meghatározó fogalom, amellyel minden rendszer – beleértve a szervezeteket is – jellemezhető.[8] A kibernetika alapfogalmai között szerepeltethető a visszacsatolás, a homeosztázis és entrópia, de meghatározó az információ és a kommunikáció is. Mindezen fogalmak az „*információ*" színes felhasználására utalnak. Bár a huszadik század közepén még alig lehetett elképzelni, de ma már biztosan tudjuk, hogy ezen meghatározások megegyeznek az információs társadalom fontosabb kulcsfogalmaival. Az információelmélet publikálása óta egy egészen új, információs társadalmi forma jött létre, amelynek központi eleme, az elektronikus rendszer és eszközei. Napjaink részévé vált ez az új technika és a munkafolyamtok szerves része, támogató pillére lett. Az informatikai hálózatra és azok eszközelire, rendszereire épített folyamatok nélkülözhetetlenek a mindennapi tevékenységben,

[6] „*Az információ tudományos és technológiai fogalom, az élet minden területén használatos. Jelent anyagszerű tudást és elvonatkoztatott lényeget, dehumanizálódik, tárgyilagos és mennyiségi.*" Az információtörténelmi modell, Vreeken, A., (2005). The History of Information: Lessons for Information Management, University of Amsterdam, Netherlands Sprouts: Working Papers on Information Systems, 5(2), fordította: Nádasi András, IKT Stratégia, Eger, 2013.

[7] Shannon, C. E., A Mathematical Theory of Communication, The Bell System Technical Journal, 1948

[8] Norbert Wiener: Cybernetics or Control and Communication in the Animal and the Machine, 1948

így a háztartásokban és az intézményekben egyaránt. Az információs rendszerekre épült világunk oly mértékű, hogy szabályozási rendszer is társult hozzá, különösen az információbiztonsági szabványok (ISO 27000 szabványcsalád) vagy néhány Európai Uniós rendelkezés, mint például a GDPR[9]. Az információs rendszer nélkülözhetetlen eleme az informatikai technológia és a hálózatelmélet, amely megjelenésével és elterjedésével immár az ipar 4.0 elnevezésű negyedik ipari forradalom korát éljük, amelynek alapeleme az információ. Az információ, valamint a digitális adat[10], és a köré épített technológia elválaszthatatlanok. A számítógép, az informatikai alkalmazások, rendszerek és hálózatok nemcsak a technológiai fejlődés aktuális állapotát tükrözik, hanem adataink védelmét is szolgálják. Ebben az értelemben nincs rangsor, *csak néhány,* nélkülözhetetlen, alapvető tényező, aminek a magja az információ és az adat, a lényege az adatbiztonság és az adatvédelem, amely a legfejlettebb informatikai megoldást kíván minden szinten.

1.2. A KUTATÁS TÉMÁJA, A TÉMAVÁLASZTÁS INDOKLÁSA ÉS A KUTATÁS CÉLJA

Az informatika kiemelt szerepét tükrözi az elektronikus kormányzati tevékenység létrejötte, a közigazgatás-tudományhoz való kötődése.[11] Az információs rendszereknek biztosítania kell az elektronikus információ rendelkezésre állását, biztonságos kezelésének lehetőségét és sértetlenségének megőrzését, amely napjaink információbiztonsági területének jelentős alapelve. Minden lánc olyan erős, mint a leggyengébb láncszeme, ez a megállapítás vonatkoztatható egy irányítási rendszerre, így annak információbiztonsági területére is. Kutatási témaként az adatvédelmi és az információbiztonsági szabványi, jogszabályi eszközök felmérését, az információbiztonság szintjének meghatározására irányuló felmérések elemzését, és a felhasználói információbiztonsági tudatosság fejleszthetőségének vizsgálatát választottam. Jogszabály szempontjából a GDPR, Infotv. és IBtv., valmaint szabvány szempontjából a ISO/IEC 27001[12] szabványra fókuszáltam, minden további szabvány és rendelkezés vizsgálata

[9] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)

[10] „*A negyedik ipari forradalom alapja a digitalizáció és az adat, a számítógép csupán eszköz*." Nagy Judit: Az ipar 4.0 fogalma, összetevői és hatása az értékláncra, Budapest, 2017

[11] az e-kormányzat társ- és határtudományai, „*Az elektronikus kormányzat alapvetően három tudományterület határán jött létre: közigazgatás-tudomány – informatika – szervezés- vezetéstudomány. Mindhárom pillére egyformán stabil és nélkülözhetetlen, bármelyiket elhagyjuk másik interdiszciplináris területre tévedünk*."
Budai Balázs Benjámin, Tózsa István: E-közigazgatás, Debrecen, 2007.

[12] Information Security Management System, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001 szabvány - Információbiztonsági Irányítási Rendszer

a háttérkutatást segítették, valamint a hipotézisek igazolásához szükségesek. A jogszabályok és a szabványok tételes vizsgálata nem része az értekezésnek. A témához szorosan kapcsolódik az információs rendszer működtetése során alkalmazandó adatvédelmi és információbiztonsági alapelvek és szabályok, az információbiztonsági kockázatkezelés, valamint a „*humán faktor*" és a felhasználói magatartás kihasználhatóságának[13] elemzése. A kutatási témám érinti az információ történeti áttekintését, az információbiztonság és vonatkozó jogintézményeit és azok fejlődését, az adatvédelmi és információbiztonsági szabályozással kapcsolatos rendelkezéseket és ajánlásokat, az információs rendszerek a felhasználói közösség számára biztosított lehetőségeit, az információs adatvagyon kezelését, különösen a személyes adatok körét, a felhasználói tevékenységet, az információs rendszerek működését befolyásoló cselekedeteket, a kártékony tevékenységeket, és az azokat előidéző tényezőket.[14] Ma már a legtöbb információmegszerzésre irányuló támadás az internetről származik. A többszintű védelmi rendszerek kialakításával törekednek teljesíteni az adatvédelmi és információbiztonsági előírásokat. A támadások rendszerint kihasználják a felhasználói hiszékenységet vagy ismerethiányt, az operációs rendszerek és alkalmazások sérülékenységét, ezért a biztonsági és védelmi megoldásokat folyamatosan fejleszteni és alkalmazni kell az incidensek megelőzésének érdekében. Egy vállalkozás vagy egy intézmény adatvédelmi és információbiztonsági szintjének mérése, a hatásvizsgálat vagy a kockázatkezelés, az objektív eredmények összehasonlítása bonyolult folyamat. Az információbiztonság elsődlegesen a megelőző eljárásokat részesíti előnybe, amelyekhez elengedhetetlen az incidensek, tehát az információfeldolgozást megszakító vagy kihasználó rosszindulatú folyamatok, a gondatlan vagy szándékos információmódosítás, illetve a jogosulatlan információfelhasználás, valamint az információs rendszer védelmi szintjének, továbbá a „*humán faktor*" felmérése, értékelése. Kutatásom során az adatvédelmi és információbiztonsági alapelvek és szabályok teljesülésén túl, mintegy kapcsolódó témakörként a felhasználói biztonságtudatos viselkedést, saját, valamint információbiztonsággal foglalkozó vállalatok, illetve kormányzati intézmények által lefolytatott kockázatfelmérésből származó adatokat vizsgálom. Kutatásom során nem

[13] Eszter Oroszi, Krisztina Győrffy: Information security for egovernment social media marketing and citizen interaction, CEEeGovDays, Budapest, 2016

[14] Ferenc Leitold, Kálmán Hadarics, Eszter Oroszi, Krisztina Győrffy, Measuring the information security risk in an infrastructure, MALWARE 2015 10th International Conference on Malicious and Unwanted Software, Puerto Rico, 2015.

foglalkoztam a kiberbiztonság és kibervédelem fogalom szerinti[15] [16] tényezőinek, az adatvédelmi és információbiztonsági incidenstípusok teljes vizsgálatával, ugyanakkor elengedhetetlen, hogy a kutatási témakörökhöz példaként adatvédelem és kibervédelem területéről származó eseteket és statisztikai adatokat prezentáljak annak érdekében, hogy az adatvédelmi és információbiztonsági rendelkezések jogalapját igazolhassam. Az incidensvizsgálat fókuszában a személyes adatokra vonatkozó adatvédelmi jogsértések, legfőképp adatszivárgás, adatlopás vagy adatvesztés, illetve néhány kártékony kódtípus által okozott incidens áll, amely során sérül különösen a titoktartás kötelezettsége, az adatok hozzáférhetősége vagy az integritás[17]. Tekintettel arra, hogy az információbiztonsági szabályozás (IBtv., ISO/IEC 27000) nagy területet foglal magába, így például a szervezet, munkavállalók, alkalmazások, fizikai biztonság, kommunikáció biztonságának és elektronikus információk védelmének területét, az értekezés terjedelmére vonatkozó korlát miatt csak azon területek kerülnek megemlítésre, amelyek a biztonságtudatos tevékenység szempontjából relevánsak. Néhány terület, mint például a kockázatkezelés hiányosnak bizonyulhat, ugyanakkor a figyelembe vettem a többi, kardinális tényezőt is. Az előbbi okok miatt a disszertáció nem érinti különösen a belső szervezetet, a fizikai és környezeti biztonság, vagy a szállítói kapcsolatok, működésfolytonosság biztosításának területét, és részben érinti az információbiztonsági szabályokat, az emberi erőforrás biztonságát, hozzáférés-felügyeletet (felhasználói felelősségek, rendszer és alkalmazás-felügyelet), titkosítás intézkedéseit, üzemeltetés biztonságát, kommunikáció biztonságát, rendszerek fejlesztését és karbantartását (kapcsolódó téma az interoperabilitási képesség kialakítása és fenntartása), információbiztonsági incidensek kezelését, megfelelést (vonatkozó jogszabályok, szellemi tulajdonjogok, magántitok és személyhez köthető információk védelme, titkosítási intézkedések) és információbiztonsági vizsgálatokat.[18] A disszertációban megemlítem a kutatásom során lefolytatott információbiztonsági kockázatkezelés eredményeit, amelyhez

[15] Krasznay Csaba, Kiberbiztonsági K+F+I Európában, Fenntartható biztonság és társadalmi környezet tanulmányok V., Sorozatszerkesztő: Kis Norbert, Koltay András, Szerkesztette: Török Bernát, Budapest, 2020.

[16] „*..a stratégia megjelöli a kibertérben jelentkező, már meglévő és potenciálisan a jövőben jelentkező fenyegetések és kockázatok rendszeres felmérését és priorizálását, a kormányzati koordináció erősítését, a társadalmi tudatosság fokozását, valamint a nemzetközi együttműködési lehetőségek kiaknázását*”
Kovács László, Krasznay Csaba, Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság 2017/1. szám, 3–16.

[17] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR), 4 cikk (12)

[18] Information Security Management System, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001 szabvány - Információbiztonsági Irányítási Rendszer, A melléklet alapján

kapcsolódik az információbiztonsági vagyonelemek kezelésére vonatkozó néhány intézkedés. Az elmúlt öt évben folytatott információbiztonsági elemzéseim és ebből származó statisztikai adataim felhasználásával további vizsgálatokat folytattam a biztonságtudatos magatartás területén, amelynek során felhasználtam az informatikai rendszerekre és a környezetünkre gyakorolt hatástanulmányokat is. Ezáltal az értekezés tartalmaz néhány évnél régebbi, de a kutatási tevékenység – beleértve a komplex vizsgán bemutatott kutatási eredményeket is – szempontjából elengedhetetlen statisztikai adatokat és hivatkozásokat (úgymint Nemzeti Adatvédelmi és Információszabadság Hatóság - NAIH, Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet - NBSZ NKI, European Union Agency for Cybersecurity - Európai Uniós Kiberbiztonsági Ügynökség - ENISA[19] statisztikai adatai, hatályát vesztett jogszabályok). A kutatási témám csak részben foglalkozik a felhasználói aktivitást kihasználó informatikai jellegű támadások és fenyegetések körével, valamint az informatikai technikai megoldásokkal, ugyanakkor fontos megjegyezni, hogy ezek a tényezők hatással vannak az adatvédelmi szabályozásra és technikai megoldásokra, az információbiztonsági szabályozásra és kockázatkezelésre, valamint a humán faktorra egyaránt. A kockázatmenedzsment tekintetében az értekezésben megtalálható, hogy milyen módszer használható a releváns fenyegetések, a támadási kísérletek vagy az incidensek elemzéséhez és kezeléséhez, de ezekre vonatkozó bővebb kutatások közlése, szintén nem része az értekezésnek. A kutatási témán keresztül vizsgálom az adatvédelmi és információbiztonsági hazai és Európai Uniós szabályozási rendszert, a fenyegetések információbiztonsági hatását, a „*humán faktort*” és a tudatosítás, valamint a digitális kultúra fejlesztésének jelentőségét, valamint egyes módszereit, ugyanakkor az értekezésben kizárólag a hipotézisek igazolásához használható módszerek és elemzések eredményeit rögzítem. A kutatási tevékenységem része a felhasználói aktivitás alapján bekövetkezett események hatásának megállapítása, lehetséges mértéke és szükséges beavatkozási intézkedések, és azok lehetséges eredményei. A kutatás szempontjából fókuszba kerültet egyes felhasználói csoportok, így legfőképp az általános felhasználó, adatkezelő, adatfeldolgozó, rendszerüzemeltető, valamint az egyetemi hallgató, illetve közoktatás tanulója. Ezen csoportok vizsgálata az incidensek általi megközelítés révén történt, mint az incidens közvetett vagy közvetlen okozója, vagy lehetséges elszenvedője. A kor és a nem meghatározása e vizsgálat szempontjából lényegtelen, mivel az incidens nem válogat, ha a lehetőségek adottak, megtörténik. A vizsgálati eredményekből kiindulva, véleményem szerint az informatikai

[19] Európai Hálózat- és Információbiztonsági Ügynökség (ENISA), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Al24153, letöltés: 2022. augusztus 7.

oktatás mellett az adatvédelmi és információbiztonsági tudatosság fejlesztésre[20] is több lehetőséget kell biztosítani. Az információbiztonsági tudatosság két meghatározó tényezője ismert, a felhasználói magatartás és az informatikai felkészültség. Egy szervezet számára elengedhetetlen különösen a polgárok azonosítása, a számítógépes eszközök biztonságos működése és kezelése, valamint az adatvédelmi és informatikai szabályok betartása, hiszen bármely területen találkozhatunk leggyengébb láncszemmel, amely sérülékenysége befolyásolja az egész szervezet működését. Az állampolgárok, akár vállalkozásban, vagy a közszolgálati szférában dolgoznak, tevékenységét vagy reakcióját, szakmai tapasztalatát közvetett vagy közvetlen módon befolyásolja az információbiztonság. Információbiztonsági tudatosság szintjének meghatározása tekintetében nemcsak a munkavállalók érintettek. Az Információbiztonsági tudatosság gyakorlat egyetemi jegyzet keretében megfogalmazott Információbiztonsági tudatosság program rámutat a felhasználói szintek jelentőségére, ugyanakkor a COVID-19 által kötelezően bevezetett távoktatási módszerek alkalmazása és azok tapasztalata a digitális kompetenciaigényeket teljes mértékben átírta. A gyerekek, és az átlag, nem informatikai szakterületen tanult, felsőfokú szakképesítéssel nem rendelkező felhasználók (5+1 szint: Általános felhasználói szint[21]) általában nem rendelkeznek azon informatikai és információbiztonsági képességekkel, amelyekkel megnyugtató módon, megfelelő szintű digitális képességgel biztosítani lehet a távoktatás háttértámogatását. A pandémia kényszerén tanulva, a gyermekeket is fel kell készíteni a virtuális világ veszélyeire, nemcsak használatának előnyeire. A rendszernek ezen hiányosságait a tapasztalatok alapján javítani szükséges, nemcsak azért, mert már az első osztályos gyermekek is okostelefont használnak, hanem mert „az adott szervezet általános felhasználóinak", azaz az adott általános iskola felhasználóinak minősülnek. Jelentős felhasználói réteg azon nyudíjasok köre is, akik a különösen a magyarországi központi azonosító (ügyfélkapu) vagy banki rendszerhez felhasználói hozzáfésrést kapnak. Az értekezésben csak azon felhasználói szintek kerülnek vizsgálat alá, amelyek az adott esemény, adat és dokumentumvizsgálat alapján kutatásom tekintetében a statisztikai mintavétel része, ezáltal például a nyugdíjasok körének vizsgálata

[20] Krisztina Győrffy, Ferenc Leitold, Anthony Arrott, Individual awareness of cyber-security vulnerability – Citizen and public servant, CEE eDem and eGov Days 2017: Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?, Budapest, 2017.05.04 -2017.05.05.

[21] „*Az információbiztonság-tudatosságnövelési program magában foglalja az adott szervezet általános felhasználóinak, kiemelt felhasználói jogokkal rendelkező vezetőinek, IT üzemeltetőinek, IT fejlesztőinek információbiztonsági tudatosítását*"
Mádi-Nátor Anett, Kardos Zoltán, Nemzeti Közszolgálati Egyetem, Mádi-Nátor Anett, Kardos Zoltán, Információbiztonság-tudatosság gyakorlat, Nemzeti Közszolgálati Egyetem, https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsag-tudatossag-gyakorlat.original.pdf, letöltés: 2022. január 18.

nem része az értekezésnek, ugyanakkor az általam megállapított általános felhasználói szint körébe tartozik. Tekintettel az adatvédelem jelentőségére véleményem szerint az információbiztonsági tudatosság fejlesztésére vonatkozó programok részévé kell tenni nemcsak az információbiztonsági, hanem az adatvédelmi alapelvek és szabályok tudatosítását is. A polgárok biztonságtudatos viselkedését a saját képességeken túl befolyásolja az információs rendszer állapota, fejlettsége, megbízhatósága, valamint a kibertér[22] adta hacker szereplőinek aktivitása, az általuk okozott kár, a jogsértések mértéke. A hackerek általában követik az IT fejlődést, és sokszor az információs védelemi intézkedések előtt járnak. A támadások megelőzésétre létrehozott többféle online oktatás[23] és útmutató[24], adatvédelmi állásfoglalás[25] segíti a felhasználói közösséget a biztonságtudatos magatartás erősítésében. Az informatikai rendszerekben a hacker által okozott kár mérhető. Gyakori, hogy helyrehozhatatlan károkat okoznak, és mindig számolni kell a járulékos veszteséggel is, amely nem minden esetben mérhető. A közszolgáltatási rendszerek fejlesztése tekintetében az egyik jelentős cél, egy olyan mértékű feltételrendszer kialakítása, amely megvalósítja a különböző közszolgáltatási szintek kiegyenlített, hatékony és biztonságos együttműködését.[26] A közszolgálati rendszerek interoperabilitásának egyik jelentős tényezője az információbiztonsági előírások betartása és rendszeren belüli, gyakorlati megvalósítása(IBtv.). A közszolgáltatási információbiztonság témához kapcsolható a Magyary Zoltán Közigazgatás-fejlesztési Program, mivel egyes fejezetében az információbiztonsági vonatkozások is szerepet kaptak. Az elektronikus közigazgatás kiterjesztésének során biztosítani kell a szolgáltatások jobb elérhetőségét, és törekedni kell az adatvédelmi és információbiztonsági alapelvek és követelmények teljesítésére. A Magyary Programban megfogalmazott magyar közigazgatás gyengeség lista (MP 11.0 végrehajtási kritika), amely szerint nem voltak elég gyorsak az eljárások, hiányzik a hatékonysági visszacsatolás, a fejlett eszközöket lassan vezetik be, túl gyorsak és felszínesek az érdekegyeztetések és hiányos a mérési és a statisztikai rendszer is. Az értekezésben is közölt kutatási eredmények figyelemfelhívók a tekintetben, hogy az információbiztonsági

[22] „*A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.*”
Magyarország Nemzeti Kiberbiztonsági Stratégiája, 2012
[23] Sans Institute, CIS Critical Security Controls, https://www.sans.org
[24] Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, IT biztonsági tanácsok, https://nki.gov.hu/it-biztonsag/tanacsok/, letöltés: 2021. április 24.
[25] Nemzeti Adatvédelmi és Információszabadság Hatóság, https://naih.hu/adatvedelmi-allasfoglalasok, letöltés: 2021. április 24.
[26] Digitális Magyarország, E-közigazgatási keretrendszer koncepció, Belügyminisztérium, 2015. április 29., Budapest

tudatosításra vonatkozó eljárások adaptálása egyes korosztályok tekintetében (digitális kompetencia fejlesztése), egyes az területeken továbbra is lassú, az exponenciálisan fejlődő IT folyamatokhoz képest. Az MP 11.0 megállapításai szerint a „… *kritikus pontok, gyengeségek nem a rossz célkitűzésből, vagy éppen emberi mulasztásból fakadnak, hanem szinte kivétel nélkül az ország és a közigazgatás teljesítőképességének korlátos voltára vezethetők vissza.*”[27] A gyengeség lista megmutatja, hogy fontos tényező a háttérszolgáltatások megerősítése, jelen esetben a zavarmentes e-közigazgatás folyamata, a sérülékenység-vizsgálat, a hiányosságok megfelelő felderítése. A közigazgatási gyengeség lista az általam felvetett hipotézisekhez is kapcsolódik, mivel a fejlettebb eszközök biztonságtudatos használatával csökkenthető a veszélyhelyzetekből eredő kockázati tényező előfordulása, alkalmazásának visszaszorítása pedig a teljesítőképesség romlásához, a kockázat mértékének növeléséhez vezethet. Bár a terület jelentős jogszabályi támogatást is kapott, az adatvédelem, az információbiztonság, a biztonságtudatosság(IBtv) jogintézményeinek bevezetése és alkalmazása terén, az értekezésben felsorakoztatott információbiztonsági statisztikai adatok, az évről évre növekvő adatvédelmi eljárások és bírságok száma rámutat a jogszabályi előírások értelmezésének és alkalmazásának hiányosságára, de legfőképp az alapelvek és szabályok figyelmen kívül hagyására. Az adatvédelmi és információbiztonsági szabályokat a jogalkotók nem azért hozzák, hogy kellő mennyiségű dokumentum legyen azok megalkotásának igazolására, hanem mert a virtuális világban legalább annyira fontos adataink biztonságos forgalomirányítása és védelme, mint személyünk védelme a valós életben, például a KRESZ által. A biztonságtudatosság hiánya adatvédelmi és információbiztonsági incidensekhez vezethet, továbbá a szabályok tudatos vagy akaratlan figyelmen kívül hagyásával a káosz eluralkodik. Az incidensek kiváltó okának bizonyítása vagy kezelése nehézkes[28], az adatvesztésért vagy adatszivárgásért senki nem akar felelősséget vállalni és esetlegesen megelégednek a bírság kifizetésével[29]. Jelenleg az Infotv. kiterjed minden olyan adatkezelésre, amely személyes adatra, valamint közérdekű adatra vagy közérdekből nyilvános adatra, ugyanakkor az IBtv. csak az állami és önkormányzati szervek elektronikus információbiztonságára vonatkozik. A hiányosság mérhető, hiszen a virtuális térben nemcsak az állami és önkormányzati szervek, hanem multivállalatok és egyetemek által

[27] Magyary Zoltán Közigazgatási-Fejlesztési Program (MP 12.0), Az elektronikus közigazgatás kiterjesztése, Budapest, 2012

[28] COUNCIL OF THE EUROPEAN UNION, COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020, amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN, letöltés: 2022. február 26.

[29] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban Ügyszám: NAIH/2020/66/21

kezelt adatok is jelen vannak. Kutatásom során megállapítottam, hogy az Infotv. által előírt hatásvizsgálat olykor kevésnek bizonyul, a kockázatkezelés az IBtv és az ISO/IEC 27001-es szabványnak megfelelő szintű elvégzése elengedhetetlen ahhoz, hogy az adott szervezet működéséhez igazított, reális kockázatelemzés szerinti, tényeken alapuló döntéshozatal megvalósuljon. Kockázatkezelés és kapcsolódó audit bizonyíték nélkül hiteles ellenőrzési eredmény sincs.[30] Az adatvédelmi és információbiztonsági jogszabályi előírások megvalósulását belső és külső kontroll folyamatokkal ellenőrizhetjük, így a rendszerauditok, az oktatási visszacsatolás által nyújtott eredmények megmutatják a kezelendő területeket, illetve a gyenge pontokat és a javítandó állapotokat. Az emberi tényező biztonságtudatossági hiányosságait kihasználó, egy jól felépített pszichológiai megtévesztési, támadási módszereket („*Social Engineering*" [31]) és technikákat 2008. óta vizsgálom. Empirikus kutatásom (interjúk, tesztek, statisztikai adat- és dokumentumelemzések) során megállapítottam, hogy a támadási kísérletek és incidensek nagy része a „*humán faktor"* gyengeségeit használja ki. A témával kapcsolatos tapasztalataimat és eredményeimet folyamatosan beépítettem kutatási tevékenységembe, így a kapcsolódó feladataimat, előadásaimat a friss ismeretanyaggal rendszeresen bővítettem. Kutatásom során az informatikai támadási formákat is vizsgáltam, ugyanakkor csak a kutatási téma szerint releváns eseményeket mutatom be részletesebben. Az informatikai technológiai megoldásokkal, mint például az ipari forradalmak vívmányai vagy a mesterséges intelligencia meghatározása[32], illetve megoldásai, valamint támadási formák részletesebb definiálásával és bemutatásával jelen értekezésben nem foglalkozom.

1.3. AZ ÉRTEKEZÉS FELÉPÍTÉSE

A disszertáció első fejezetben rögzített hipotézisek igazolására szolgáló kutatási folyamatban informatikai és információbiztonsági módszerek, valamint közigazgatástudományi elméletek, továbbá Magyarország, valamint az Európai Unió által deklarált jogszabályok segítségével vizsgálom és összegzem a kutatásommal kapcsolatos, releváns információkat, statisztikai adatokat és megállapításokat, amelyek alátámasztják vagy elvetik a felállított feltételezéseimet.

[30] Részletesebben megtalálható a 3.1.1 Adatvédelmi jogsértések fejezetében, A hamburgi (német) felügyeleti hatóság az általános adatvédelmi rendelet 66. cikkének (2) bekezdése szerinti, a Facebook Ireland Limitedre vonatkozó végleges intézkedések elfogadásának elrendelésére irányuló kérelméről szóló 01/2021. sz., sürgősségi eljárás keretében elfogadott kötelező erejű határozat, Európai Adatvédelmi Testület, kötelező erejű határozata, Elfogadás időpontja: 2021. július 12., https://edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_hu, letöltés: 2022. július 21.

[31] Kevin D. Mitnick, William L. Simon: The art of deception, 2003

[32] Kovács László, Czékmann Zsolt, Rító Evelin, A mesterséges intelligencia alkalmazásának lehetőségei az államigazgatásban, Infokommunikáció és Jog, 2020/2. (75.), e-különszám

A megállapítások, a tényeken alapuló döntéshozatal[33] alapelv gyakorlatára épül, amelyek vélhetően kielégítik a hipotézisek igazolásának követelményeit. A jelen disszertáció kísérlet arra vonatkozóan, hogy a feltételezések igazolásához szükséges információbiztonság, a közigazgatás és a magánszféra adatvédelmének jelenlegi helyzetét bemutassam, az információbiztonsági tudatosság szempontjából elemezhessem és az információbiztonsági tudatosság és az adatvédelem, illetve az információbiztonság közti összefüggéseket feltárhassam annak érdekében, hogy az információbiztonsági tudatosság hiánya, a kockázati tényezők és fejlesztési lehetőségek megállapításra kerüljenek, és ezáltal a magyarországi digitális kompetenciafejlesztést támogassam. A disszertáció fő témája az információbiztonsági tudatosság helyzetének és fejlesztési lehetőségeinek vizsgálata, amelyhez szorosan kapcsolódik az információtörténeti és adatvédelmi jogtörténeti áttekintés, információbiztonsági események és statisztikai adatok elemzése, információbiztonsági kockázatkezelés, valamint a „*humán faktor"* és a digitális kompetencia fejlesztését befolyásoló tényezők áttekintése.

Az értekezés figyelembe veszi

- az információtörténeti és adatvédelmi jogtörténeti szempontból a preindusztriális, indusztriális és a posztindusztriális társadalom formális jellemzőit, az információvédelmi megoldásokat, az adatvédelemmel kapcsolatos jogintézmények kialakulását, a szerzői jogtól az adatvédelemig és az információbiztonságig (a téma szempontjából jelentős tényezők vizsgálata az Ókortól napjainkig),
- az adatvédelmi és információbiztonsági szabályozás terén az emberi jogok és alapvető szabadságok védelméről szóló római Egyezmény (EJEE) elfogadásától, a napjainkban érvényes és hatályos, a téma szempontjából releváns hazai és Európai Uniós adatvédelmi és információbiztonsági jogszabályi rendelkezéseket (1950-2021. időszakra vonatkozóan),
- az adatvédelmi és információbiztonsági események, felmérések statisztikai adatait, valamint a vonatkozó hatósági határozatokat és az incidensekből eredő következtetéseket (2000-2021. időszakra vonatkozóan),
- az információbiztonsági kockázatfelmérés és kockázatkezelés statisztikai adatait és következtetéseit (2015-2021. időszakra vonatkozóan),
- a balesetek „*humán faktorra*" vonatkozó vizsgálatok és kutatási adatait (1990-2020. időszakra vonatkozóan),

[33] MSZ EN ISO 9001:2015 Minőségirányítási rendszerek, Követelmények

– a digitális kompetencia fejlesztésére vonatkozó követelményeket (2017-2021. közötti időszakra vonatkozókat).

Tekintettel a disszertációban szereplő téma jelenlegi aktualitására és dinamikusan változó tényezőire, szeretném kiemelni, hogy a disszertáció kutatási dokumentumainak feldolgozását és összegzését 2022. február hónap végén, az előbírálatok szerinti módosítást 2022. augusztus hónap elején fejeztem be, a következtetéseket és hipotézis igazolásokat, valamint a tudományos eredményekre vonatkozó megállapításokat a 2022. március hónap végén rendelkezésemre álló statisztikai adatok és dokumentumok alapján fogalmaztam meg. Az információ és ennek megfelelően az információbiztonság jelenleg az adatvédelmi szabályozáshoz kapcsolható, de jelen van minden egyes tudományterületen, a társadalmi, gazdasági és kulturális élet szerves része. Az információ, így az információbiztonság nem szakítható el egyik területtől sem. Valós jelentése viszont csak akkor kaphat értelmet, ha behatároljuk és valamely tudományághoz illesztve vizsgáljuk. Véleményem szerint jelen kontextusban a személyhez, a közigazgatáshoz és az államigazgatáshoz vonatkozóan kell vizsgálni, így nemcsak a szellemi alkotások joga, a személyi jogok, az adatvédelem, a GDPR kerül előtérbe, hanem a közigazgatási és államigazgatási információk, amelynek része lehet például az államtitok, nemzetvédelmi információk, közigazgatási nem publikus, közérdekű, valamint a közérdekből nyilvános adat. Az értekezésnek nem témája az adatvédelmi, az információ-, valamint az információbiztonsági kategóriák, alapelvek, szabályok és események teljes palettájának felsorakoztatása és vizsgálata, valamint minden meghatározás bemutatása, de a téma szempontjából a legrelevánsabb területek és szakkifejezések megvilágításra kerülnek.

1.4. A TÉMA VIZSGÁLATÁNAK HIPOTÉZISE, A KIDOLGOZÁS SORÁN ALKALMAZOTT MÓDSZEREK

1.4.1. A TÉMA VIZSGÁLATÁNAK HIPOTÉZISE

A kutatás alatt folytatott eddigi tevékenységem során az alábbi hipotéziseket fogalmaztam meg:

– Az első hipotézisem (H1) szerint feltételezem, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és jogszabályi rendelkezések fejlődése a nemzetközi szabványügyi intézmények ajánlásaival és az európai szabályozással összhangban vannak.

- A második hipotézisem (H2) szerint feltételezem, hogy a felhasználói információbiztonsági tudatosság hiánya elősegíti az adatvédelmi jogsértések bekövetkezését, ezáltal kiberbűnözést.
- A harmadik hipotézisem (H3) szerint feltételezem, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését.
- Az negyedik hipotézisem (H4) szerint feltételezem, hogy az információbiztonsági tudatosítás rendszerét nemcsak az informatikai oktatásban, hanem minden korosztály számára elérhetővé kell tenni és minden szakterületen indokolt bevezetni és működtetni.

A H1 hipotézis igazolásának tekintetében a vonatkozó jogtörténet, történeti áttekintés, adatvédelmi és információbiztonsági szabályok, és szabványok vizsgálata (második fejezet) nélkülözhetetlen. A kutatási terület szempontjából elsősorban a téma pozícionálása, a releváns adatvédelmi és információbiztonsági szabályozás folyamatainak vizsgálata és kapcsolatok elemzése szükséges abból a célból, hogy az információbiztonsági tudatosság helyzetét a törvényi előírásokhoz mérten vizsgálhassam. Tekintettel arra, hogy Hazánk az Európai Unió tagállama, számos Uniós jogszabálynak, így az általános adatvédelmi rendelet előírásainak is meg kell felelnünk, ezáltal a vizsgálat fókuszát ki kell terjeszteni a nemzetközi, de legfőképp az Uniós jogrendre, a tekintetben, hogy Hazánk a szabályozási kötelezettséget milyen szinten teljesíti és szabályozásunk mennyire illeszkedik a nemzetközi gyakorlatba, illetve más tagállam, például Németország hogyan valósította meg vonatkozó feladatait. A szabályok vizsgálata azért fontos, mert a jogalkotói, tehát adatvédelmi és az információbiztonsági elvárásoknak megfelelően védik és biztosítják az állampolgárok adatvédelmi jogait, egyértelműen rögzítik az adatkezelők és adatfeldolgozók kötelezettségét, alkalmazásuk korlátozhatja az adatgyűjtést, csökkentheti az adatvédelmi incidensek számát, valamint növeli az információs rendszerek információbiztonsági szintjét, és a rendelkezések alapján az adatvédelmi jogsértések szankcionálhatók. A szabványok alkalmazásával az információs rendszerre vonatkozó bizalmasság, sértetlenség, rendelkezésre állás, valamint az adatvédelmi alapelvek teljesülnek, aminek következménye a tudásra, az információra, az intellektuális technológiára épített bizalmasság növelése, továbbá a posztindusztriális társadalom fejlődése.

A H2 hipotézis szerint a felhasználói információbiztonsági tudatosság hiányának hatása esetlegesen az adatvédelmi jogsértés. A vizsgálat tárgya elsődlegesen a H1 és H2 hipotézis ok-okozati összefüggése, a H1 és H2 hipotézis során vizsgált folyamatok és hiányosság eredményei, úgymint a szabályok be nem tartásának következményei, valamint az

információbiztonsági tudatos, szabálykövető és a szabályszegő magatartás összefüggéseinek tanulmányozása, beleértve az információbiztonsági tudatosság hiányainak és a kiberbűnözés lehetőségeinek korrelációját (H2). Tekintettel arra, hogy az adatvédelmi jogsértések és eljárások, valamint a kiberbűnözések száma és az ebből eredő anyagi kár évről-évre növekszik, amely alapján indokolt az információbiztonsági szabályok alkalmazása nemcsak az állami és az önkormányzati szervek, hanem a gazdasági társaságok tekintetében egyaránt. (az igazoláshoz elsődlegesen a harmadik, de a negyedik és ötödik fejezetek statisztikai adatai is relevánsak)

A H3 hipotézis igazolásának tekintetében a kutatás tárgya a H2 hipotézis vizsgálata során kapott eredmények összevetése az információbiztonsági kockázatkezeléssel és a tudatosításra fókuszált intézkedések eredményességével, a „*humán faktor*" és az információbiztonsági kockázatkezelés összefüggéseinek vizsgálata. A H2 és H3 hipotézis igazolása átfedéseket eredményez a „*humán faktor*" hatás vizsgálatának tekintetében.

A H4 hipotézis vonatkozásában a H2 és H3 hipotézis igazolása során kapott eredmények alapján a vizsgálat tárgya a digitális kultúra állapota, az információbiztonság-tudatosságnövelési program, annak hatékonysága, a program alapján további információbiztonsági-tudatossági szintek meghatározása, és a témákban érintett korosztályok vizsgálata. A H4 hipotézis igazolásánál az Európai Unió digitális kompetencia javaslatait is figyelembe veszem.

A fentiekben található hipotéziseket a következő elméletet szerint igazolom. Az adatvédelmi és információbiztonsági incidensek számának növekedése, valamint a hazai adatvédelmi és az információbiztonsági rendelkezések fejlődése évről évre intenzívebb, ugyanakkor az információbiztonsági oktatási módszerek kidolgozása és alkalmazása lassabb fejlődést mutat. Kutatásom során kapott eredmények bemutatásával igazolom, hogy az emberi hibák és azok következményeinek száma csökkenthető az információbiztonsági-tudatosság fejlesztési rendszer bevezetésével. Az informatikai technológiák, valamint az információs társadalom fejlődése és az adatvédelmi és információbiztonsági szabályozás hatással van egymásra. Ezen összefüggések információbiztonsági vizsgálata lehetőséget ad az empirikus, szubjektív következtetések összegzésére és a statisztikai adatok értékelésére. Az értekezésben bemutatásra kerülnek a kutatás szempontjából releváns módszerek, adatvédelmi, és kiberbűnözési statisztikai adatok, amelyekkel a hipotéziseket kívánom igazolni. Információbiztonsági felméréssel megállapítható az információs rendszer biztonsági szintje és elemezhető a biztonságtudatos magatartás. Az emberi akaratlagos vagy akaraton kívüli magatartásból eredő

kár az információbiztonsági kockázatkezelés módszereivel kimutatható, és hatása, valamint nagysága mérhető. Az emberi magatartás többféle módszerrel befolyásolható. A pozitív eredmény és a vonatkozó információbiztonsági maradványkockázat csökkentésének érdekében különböző információbiztonsági tudatosításra vonatkozó módszerek alkalmazhatók. Kimutatható továbbá az összefüggés a felhasználói társadalom viselkedése, az informatikai tudomány fejlődése és az információbiztonsági kockázat között. Ennek igazolására szolgál különösen a disszertációban említett feltételezések, és az adatvédelmi incidensek elemzése, valamint a statisztikai kimutatások összevetése. A hipotézisek kifejtéséhez és a kérdések megválaszolásához elengedhetetlenül szükséges az adatvédelmi alapelvek bemutatása, a nemzetközi és a hazai adatvédelmi jogtörténete, valamint az információbiztonság fogalomrendszerének, jogintézményének, környezetének és kapcsolódó történeti tényezők vizsgálata. Az adatvédelmi és információbiztonsági jogtörténeti áttekintés előkészíti a hipotézisigazolásokat és segítséget nyújt a mai jogszabályok értelmezésében, az adatvédelmi jogsértések, valamint az információbiztonsági incidensek elemzéséhez és a következtetések meghatározásához. Az értekezésem végeredményéül kapott állításokkal erősíteni szeretném azt a feltevést, hogy az adatvédelmi és információbiztonsági alapelvekre épített felhasználói információbiztonsági tudatosság növelése nagymértékben hozzájárul az információs rendszereink – és ebben az esetben legfőképp a hazai közszolgálati rendszerek – megerősítéséhez, míg a hiánya vagy gyengesége az információs rendszereink gyenge pontjait növeli, ezáltal az információs rendszer sérülékenyebbé, kihasználhatóbbá válhat. Az értekezésben ismertetett adatvédelmi és információbiztonsági incidensek, valamint azok elemzései, a következtetések igazolják a rendeletekben és törvényekben, valamint egyéb rendelkezésekben szükségszerűen megfogalmazott adatvédelmi és információbiztonsági alapelveket és előírásokat.

1.4.2. A KUTATÁS SORÁN ALKALMAZOTT MÓDSZEREK

A kutatásom során többféle kutatási módszert alkalmaztam, amelyeket az alábbiaknak megfelelően csoportosítottam:

- dokumentum- és tartalomelemzés kvalitatív, minőségirányítás módszerek, összehasonlító elemzés,
- statisztikai adatok elemzése, források, adatbázisok vizsgálata,
- kvantitatív módszerek,

- empirikus kutatás, az észszerűség, a matematikai logika alkalmazásával, valamint az objektív és pontosságra törekvő megfigyeléssel, továbbá
- a kutatás szempontjából releváns és egységes fogalommeghatározás, tekintettel arra, hogy a kutatásom konzekvens fogalomhasználatot kíván, ezért szükségesnek tartom bemutatni és meghatározni a kapcsolódási pontokat. [34]

A fenti csoportoknak megfelelően a kutatási tevékenységem alatt alkalmaztam az említett módszereket különösen, az információtörténet kutatása, adatvédelmi és információbiztonsági jogtényezők, jogtörténet kutatása, továbbá a szubjektív mintavételezés, kockázatkezelés[35], valamint kutatásom során kapott statisztikai adatok elemzése, és statisztikai adatok kiértékelése során. Az említett módszereket felhasználtam tehát az információtörténet kutatásom alkalmával, az adatvédelmi és információbiztonsági jogtényezők, valamint témához kapcsolódó jogtörténet vizsgálatánál, amely általános és összehasonlító jellegű kronologikus elemzés, legfőképp jogszabályi és jogtörténeti tényezők feldolgozására. A kutatásom ezen részére vonatkozó eredmények a második fejezetben találhatóak. A történelmi áttekintés során különösen az információ, az adatvédelem, az információbiztonság történeti és jogtörténeti elemzésre koncentráltam.[36] [37] [38] A személyhez fűződő jogok tekintetében fókuszba került a szellemi jogok kialakulása és története is (2. melléklet, A szellemi alkotások jogtörténete és védelme), amelyen keresztül rávilágítottam arra, hogy a szellemi tulajdon az alkotás terméke, így eredetét tekintve kizárólag az egyént illeti, jogi személyt nem. A szubjektív mintavételezés során az értekezésben megfogalmazott hipotézisek igazolásának érdekében olyan adatokat és esettanulmányokat elemeztem, amelyek a téma szempontjából relevánsak. Az érintett jogszabályokhoz kapcsolódó irányelvek kialakulására vonatkozó kutatásom érintette különösen a nemzetközi és hazai adatvédelmi irányelveket és alapelveket, egyezményeket, ezáltal a nemzetközi, de elsősorban Európai Uniós, valamint példaként németországi, továbbá a hazai adatvédelmi törvényeket és rendelkezéseket, a nemzetközi információbiztonsági ajánlásokat, valamint a hazai információbiztonsági törvényeket és rendelkezéseket. A statisztikai adatok

[34] Bella Tamás, A kutatási módszer és mintavétel megválasztása a tudományos kutatásokban, A magyar természettudományi társulat tudománytörténeti kötetei II., pp. 247-263.o., DOI 10.23716/TTO.22.2018.18, Budapest, 2018.
[35] Information Security Management System, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001 szabvány - Információbiztonsági Irányítási Rendszer
[36] Halász Iván, Wenzel Gusztáv és a magyar jogi komparatisztika kezdetei, Pro publico bono - Magyar közigazgatás 3. sz., 2015. 152-162. oldal (összehasonlító jogtörténet)
[37] Máthé Gábor, A hatalommegosztás kérdései, Jogtörténeti szemle 2. sz., 2004. 44-47. oldal
[38] Máthé Gábor, Intézménytörténet és jelenkor, Jogtörténeti szemle 3. sz., 1990. 103-105. oldal

gyűjtésére és elemzésére vonatkozó kutatásom elsősorban az adatvédelem[39] területéről valamint az információbiztonság (kibervédelem)[40] területéről származó, statisztikai adatokra épült. Az információbiztonsági kutatás során alkalmazott módszereket a kockázatkezeléshez, az intézkedési tervek összeállításához, a biztonságtudatosság állapotának és változásának mérésére használtam fel. A stratégiai módszereket az információbiztonsági-tudatosság fejlesztésének megvalósíthatóságához alkalmaztam. Az analízis, szintézis módszereire épülő helyzetelemzést és -értékelést az adatvédelmi és az információbiztonsági statisztikai kutatáshoz és kockázatkezeléshez használtam fel. A kutatási részeredmények megvitattam tudományos fórumokon és tudományos konferenciákon is. Érvek és ellenérvek vizsgálatának tényezőit és eredményeit beépítettem mind a kutatói munkámba, továbbá az értekezésben is szereplő részeredményekbe, amelynek összefoglalása a fejezetek végén megtalálhatók. További eredményeket saját publikációimban is közöltem (publikációs jegyzékem). Véleményem szerint a kapott részeredmények alkalmasak a hipotézisek igazolására vagy cáfolására, valamint az empirikus módszerek alapján az értekezés reális, tudományos eredményeinek összegzésére. A fent említett módszereket legfőképp a második, harmadik, negyedik és ötödik fejezetnél használtam fel. A kutatásom tehát többféle módszert érint, amelyek közül az információbiztonsági módszereket az alábbiaknak megfelelően csoportosítottam: információszerzési módszerek (különösen összehasonlító elemzések, megfigyelések, és adatbányászat alkalmazása, elsődlegesen adatvédelmi és információbiztonsági jogtörténet, incidensvizsgálat és kártényezők összegyűjtésére és kiértékelésére), felhasználói közreműködést igénylő fenyegetés- és támadásvizsgálatokra irányuló információszerzési módszerek (különösen megfigyelési és mintavételezési módszerek), kockázatelemzési módszerek (különösen mintavételezési, kvalitatív és kvantitatív módszerek alkalmazása). A megfelelően megtervezett és megalkotott kockázatkezelés értékteremtő és védi a vagyonelemeket, adatot szolgáltat a katasztrófa-elhárítási terv meghatározásához, ezáltal biztosított az informatikai fejlesztési terv teljesítése, elősegíti az informatikai szervezet folyamatos fejlődését, növeli az informatikai hatékonyságot, megalapozza a döntéshozatalt,

[39] Különösen az adatvédelmi állásfoglalásokban szereplő megállapítások, nemzetközi (Európai Adatvédelmi Testület, EDPB) és hazai adatvédelmi (Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH), valamint információbiztonsági incidensek (Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, NBSZ NKI, IT biztonsági sajtószemle): adatszivárgások és okozott károk, adatvédelmi határozatok, adatvédelmi hatósági eljárások, nemzetközi és hazai adatvédelmi bírságokról szóló határozatok és publikációk.

[40] Elsődlegesen a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, NBSZ NKI, IT biztonsági sajtószemle adatai, valamint nemzetközi információbiztonsági incidensek alapján készített statisztikai elemzések, továbbá információbiztonsági útmutatók adatainak elemzése alapján készítettem. Kiemelendő, hogy a NBSZ NKI statisztikai adatai az IBtv. vonatkozásában érintett területről származnak.

valamint elkerülhetők a kedvezőtlen események. Az értekezésben rámutatok arra, hogy az alkalmazott kockázatkezelési módszerek segítségével összetett felmérés készíthető egy intézmény biztonságtudatossági szintjével kapcsolatban. Az információbiztonsági kockázatkezelés rávilágít az informatikai biztonság gyenge pontjaira, továbbá módszerek és mérőszámok segítségével olyan hasznos megoldásokat állíthatók elő, amelyeket a szervezet tekintetében elemezve és felhasználva pozitív eredményeket lehet elérni. Nemcsak egy felmérési módszer segítségével tesztelhető a felhasználók információbiztonsági ismerete. Az értekezésben felsorolt módszerek és esettípusok elláthatók mérőszámmal, és elemezhetők, valamint az említett technikák és a kockázatelemzési módszerek együttesen alkalmasak arra, hogy a jelen kutatás egy-egy eredményét képezzék. Az egyes kockázatelemzési technikák ismertetése és az esetek bemutatása és értékelése, a biztonságtudatosság fejlesztési és információbiztonsági módszerek alkalmazása, az összefüggésének azonosítására és a fejlesztési javaslatok kidolgozására szolgál. Kutatásom alkalmával az információbiztonság területén nemcsak a rendszerek biztonságával, sértetlenségével és rendelkezésre állásával foglalkoztam, hanem a szellemi alkotásokkal, a személyes adatokkal, azok biztonságával, valamint a biztonság kialakításához kapcsolódó oktatási, a tudatosítási módszerekkel. A tapasztalatom azt mutatja, hogy nem elég a felnőttoktatásban elkezdeni a tudatosítást, hanem már gyerekkorban érdemes felhívni a figyelmet, és a gyerek-szülő-pedagógus együttes tájékoztatása, valamint a résztvevők együttműködése eredményes megoldás lehet. Természetesen a felhasználók másik körét, a kritikus rendszert üzemeltető adminisztrátorokat és a rendszerüzemeltetőket sem szabad kihagyni az oktatásból. A legegyszerűbb felhasználói név – jelszó, azaz a password policy tudatosításától a rendszerek, hálózati eszközök menedzseléséig széles az oktatási, a biztonsági oktatás és kutatás skálája. A témában született és hivatkozott publikációk is ezt igazolják. A hivatkozott publikációk egyrészt közigazgatási szabályozásra, másrészt általános információbiztonsági sebezhetőségekre és esetleges megoldásokra hívja fel a figyelmet. Véleményem szerint, biztonságtudatosság szempontjából vizsgálat alá kell vonni a lehető legteljesebb területet, majd részletesebben kell megvizsgálni a legkritikusabb és a kutatási témához legközelebb eső terület szeletét. Az értekezés tekintetében ezt az elvet szeretném követni. A kutatásom során nemzetközi és hazai tudományos publikációk, hatóságok és adatvédelmi, valamint kibervédelmi statisztikai adatgyűjtéssel és adatfeldolgozással foglalkozó vállalatok által nyilvánosságra hozott, hiteles statisztikai adatait gyűjtöttem össze, dolgoztam fel és vizsgáltam, annak érdekében, hogy hipotézisem adatvédelmi és információbiztonsági tényezőit hitelesen igazolni vagy cáfolni tudjam. Tekintettel arra, hogy kutatásom során az

információbiztonsági tudatosság hiányát, annak kiváltó tényezőit és következményeit vizsgálom, a digitális kompetencia állapotára irányuló eredmények megállapításához és fejlesztési igények összegzéséhez már nem elegendő az egyszerű, lakossági kérdőíves módszer alapú megállapítás, hanem elsősorban a hatóságok által összeállított hiteles adattartalmon alapuló statisztikai elemzés szükséges. Összehasonlítva a lakossági kérdőíves módszer és a hatósági vizsgálatokból eredő, statisztikai adatokon alapuló lehetséges eredményeket, kutatásomhoz a hiteles adatforrásokon alapuló kutatást és eredmények kiértékelését tartottam előnyben. A hatósági statisztikai adatelemzést összevetettem információbiztonsági auditorként végzett, saját kutatási, statisztikai adataimmal. Mindkét elemzés során hasonló eredményeket kaptam, amelyet az összegző megállapítás, következtetések fejezetében igazolok. Véleményem szerint az értekezésben közzétett kutatási eredményeim, úgymint az adott szervezet tekintetében megállapított, információbiztonsági kockázatkezelésből származó, valamint a NAIH nyilvános határozataiból és éves beszámolóiból, és az NBSZ NKI által kezelt és havonta nyilvánosan közzétett (IT Biztonsági Sajtószemle, 2017-2021. időszakra vonatkozóan) incidensekre vonatkozó adatokból általam összeállított statisztikai eredmények alkalmasak arra, hogy az általam felállított hipotézisek megfelelő igazolást nyerjenek.

2. AZ INFORMÁCIÓ JELENTŐSÉGE, AZ ADATVÉDELEM ÉS AZ INFORMÁCIÓBIZTONSÁG JOGTÖRTÉNETE ÉS SZABÁLYOZÁSI RENDSZERE

2.1. AZ INFORMÁCIÓ JELENTŐSÉGE

Történelmünk több ezeréves időszaka alatt sokáig nem tulajdonítottak jelentőséget a mai értelembe vett információ fogalmának és az információbiztonság szabályozási rendszer kiépítésének. Bár az információ jelentőségét és a tudást nem becsülték alá, mégis az információbiztonsági intézkedések legfőképp technikai jellegűek voltak, és a fellelhető tudományos értekezések is leginkább az „ideák" vagy a szellemi alkotások eszméit világítja meg. Az ókori társadalmak, sőt a filozófia nagy mesterei talán kevésbé foglalkoztak az információ által betöltött jelentőségre, birtoklásának következményére, így előnyére vagy hátrányára. Az elektrotechnikai fejlődés, az információelmélet kutatásának eredményei és az informatikai technológia, valamint a paradigmaváltás a különböző tudományágakban a korábbi évszázadok „nyugalmas" életviteléhez képest oly mértékű információrobbanást okozott, amely az ipari forradalom negyedik állomásához vezetett, és ipari, társadalmi, kulturális változásokat eredményezett. Az információbiztonság túlmutat egy divatos kifejezésen, és a vonatkozó szabályok felállítása és alkalmazása jelentősen befolyásolja az információs rendszerek működését. Napjainkban az információs társadalomban a rendelkezésre álló információs rendszerek és szolgáltatások létfontosságú szerepet játszanak mind a háztartásokban, mind az üzleti életben, ezért megbízhatóságuk és biztonságuk lényeges szempont. A biztonsági események nagyságrendje, gyakorisága és hatása évről évre, mondhatjuk, exponenciális mértékben növekszik, ami súlyos fenyegetést jelenthet az információs társadalom működésére és tevékenységére. Az információs rendszerek a működésük akadályozására, károkozására vagy adatainak felhasználásával jogtalan haszonszerzésre irányuló szándékos és ártalmas cselekmények célpontjaivá válhatnak. Az informatikai incidensek nehezíthetik a mindennapos életet, a gazdasági tevékenységek gyakorlását, jelentős pénzügyi veszteségeket, valamint bizalomvesztést és súlyos károkat okozhatnak az európai közösségnek és a gazdasági tevékenységeknek.[41]

[41] Győrffyné Holló Krisztina: Az információbiztonság jelentősége és története, GRADUS Vol 8, No 2 (2021), John von Neumann University, Hungary, Kecskemét

Ez a fejezet az első hipotézisem (H1) bizonyításához szükséges kutatási eredményeket tartalmazza. A H1 hipotézis szerint feltételeztem, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és jogszabályi rendelkezések fejlődése a nemzetközi szabványügyi intézmények ajánlásaival és az európai szabályozással összhangban vannak. Kutatásom során megvizsgáltam a nemzetközi (Európai Uniós) és a hazai adatvédelmi (elsődlegesen a GDPR, mintaként a német szövetségi adatvédelmi törvény, és hazai vonatkozásként az Infotv.) és az információbiztonsági rendelkezések (IBtv.) és szabványi ajánlások (ISO/IEC 27001) jelentőségét és az adatvédelmi alapelvek, valamint szabályok alkalmazásának szükségességét. A kutatásom eredményét, a jelen fejezetben bemutatott módon, az adatvédelmi és információbiztonsági jogtörténet vizsgálatának kivonatával, az összehasonlító elemzési módszerének figyelembe vételével igazolok.[42] [43] [44] Ebben a fejezetben található eredmények kifejtéséhez és a háttérkutatáshoz dokumentum- és tartalomelemzési, kvalitatív, összehasonlító elemzést, adatbázis és statisztikai elemzéseket használtam.

2.2. AZ INFORMÁCIÓTÖRTÉNET, KULTURÁLIS ÉS TUDOMÁNYOS NÉZETEK FEJLŐDÉSE

Az információ jelentőségének feltárása lehetőséget ad arra, hogy az informatika világát kiszélesítve, jelentését is kibővítsük. Az információ eredetét tekintve már az ókor nagy filozófusai is foglalkoztak a témával, de Platón és Arisztotelész összekapcsolta az információ fogalmát a lételmélettel. Bár jelen álláspontok szerint információtartalommal bír az adat, jel és a kód is, amennyiben visszatekintünk az idő vonalán megállapíthatjuk, hogy valójában latin eredetű, értesülést, hírt, üzenetet, tájékoztatást jelent, és az „*informare*" és „*informatio*" szavakból származik. Az információ jelent olyan új ismeretet, amely megszerzője számára szükséges, és a korábbi tudása alapján értelmezhető, vagy olyan tényt, amelynek megismerésekor olyanfajta tudásra teszünk szert, ami addig nem volt birtokunkban. Az „*informare*" szó jelentése szerint az anyag vagy értelem formálása, filozófiai, morális és pedagógiai (oktatni, nevelni) szempontból. Az „*informatio*" magára a folyamatra utal. Ebben a kontextusban a „forma" úgy szerepel, mint lehetőség a tudás megszerzésére. Ezeket a szavakat a megfogható és a megfoghatatlan filozofikus szövegkörnyezetben gyakorta használták. Platón *Phaidón* (Kr. e. V. század, Kr. e. 427 – Kr. e. 347) című művében közölt vélekedései és

[42] Halász Iván, Wenzel Gusztáv és a magyar jogi komparatisztika kezdetei, Pro publico bono - Magyar közigazgatás 3. sz., 2015. 152-162. oldal (összehasonlító jogtörténet)
[43] Máthé Gábor, Intézménytörténet és jelenkor, Jogtörténeti szemle 3. sz., 1990. 103-105. oldal
[44] Máthé Gábor, A hatalommegosztás kérdései, Jogtörténeti szemle 2. sz., 2004. 44-47. oldal

magyarázatai során, a következő célt tűzi ki: „*Ha valaha is tisztán akarunk tudni valamit, el kell a testtől szakadnunk, és csupán a lélekkel kell szemlélnünk a dolgokat önmagukban, és akkor minden valószínűség szerint a miénk lesz, amire vágyunk, s aminek, mint valljuk, szerelmesei vagyunk: az eszmélet*”[45] [46]. Művében megjeleníti a belső formát, az „*idea*”-t, „*eidosz*”-t (forma, alak). Vélekedése szerint minden tudásunk valójában egy lelki visszaemlékezés, mivel nem származtathatunk mindent a tapasztalatból, már korábban ismernünk kellett. Összességében mindez az új dolgok megismerésének és a meglévővel egyesítésének elméletére utal. Az Ókor másik nagy filozófusa, Arisztotelész *A lélekről* című műve két évezredre meghatározta a lélekfilozófiát. Radikális ismeretelméleti tézise szerint „*a lélek bizonyos módon azonos valamennyi létezővel*”, mégpedig úgy, hogy az értelmes lélekrész alsóbb része, az ún. passzív értelem, a megismerés során azonosul a megismert dolog „*belső formájával*”, szubsztanciájával. Ez az azonosulás a lélek (mely maga is forma, a test belső formája) belső megformálódása, az információ. Ezt az információ-fogalmat a filozófia ma is használja.[47] A középkorban is alkalmazták az „*informatio*" és "*informo*" szavakat, mégpedig a skolasztikusok, a hylomorfizmus tanok megvitatása során. Az elméletek szerint a dolgok formából és anyagból állnak össze. A forma alakítja (in-form), formálja az anyagot, az anyag megvalósítja a formát, tehát a két fogalom tartalma között kölcsönös kapcsolat alakult ki. Ez az elmélet számos késő-középkori vallásnak és tudománynak volt az alapelve. Az „információ” ebben a korszakban egy összetett fogalom, ami utal egyben a világegyetem rendjére és szerkezetére, és a materiális dologra is. Két angol szó is megjelent ebben az időben, a 14. század végén, mégpedig az „*informe*" és az „*informacioun*". Mindkét fogalom rendelkezett már az arisztotelészi hylomorfizmus hatásával.[48] Arjan Vreeken amszterdami Egyetem kutatója által megalkotott információtörténeti modell (1. táblázat) megfelelően összefoglalja a különböző korszakok információ jelentéstartalmát, lételméleti és ismeretelméleti kapcsolatát, így az információ fogalmi fejlődését az elmúlt évszázadokban.

[45] „eszmélet” helyett itt belátás és tudás
[46] Platón összes művei I., Kerényi Grácia fordítása, Európa, Budapest, 1984
[47] Vassányi István, Információelmélet jegyzet, Veszprémi Egyetem (Pannon Egyetem), Műszaki Informatika Kar, 2002-2012
[48]. Wilhelm Gábor, Antropológiai tárgyelmélet, Pécs, 2010„*A hylomorfizmus értelmében minden egyedi konkrét individuum, dolog anyag és forma „kombinációja*””

Arjan Vreeken információtörténelmi modellje alapján		Lételmélet	Ismeretelmélet
Korszak	**Jelentés**	**a) Az anyag alakításának folyamata b) A forma**	**a) Az értelem alakításának folyamata b) A tudáshoz való viszony**
Latin korszak Kr. e. I. sz. -Kr. u. XI. sz.	Az információ szerepe, hogy közvetítse a görög (filozófiai) fogalmakat és jelentéseket, a forma kialakuljon (anyagrész), és közvetítse a szükséges folyamatokat is.	a) Az anyag formába öntése b) Az idea és a tiszta forma	a) Az értelem "formálása" b) A forma, mint a tudás lehetősége
Skolasztikusok XII-XVI. sz.	A sklolasztikus hylomorfizmus keretein belül, a világegyetem alakíthatósága.	a) A világegyetem tevőleges alakulása b) Metafizikai forma	a) Az értelem "formálása" b) Érzék és értelem
Újkor kezdete XVIII-XIX. sz.	Az ember empírikus megismerése, tárgyilagos, érzékek általi megismerés, az ész és az érzékek formálása.	a) A sklolasztikus lételmélet elavulttá válik b) Elavult	a) Az ész és az érzékek formálása b) Az érzéki megismerés érzéki tudást ad
Állami bürokrácia XIX. sz.	Az állam ellenőrzése és a bürokrácia, az információ jelentése: az anyagszerű tudás és emberi megismerhetőségen túl.	a) Elavult b) Elavult	a) Elavult b) Anyagszerű tudás, emberi nélkül
Modern információs társadalom kezdete XX. sz.	Az információ tudományos és technológiai fogalom, az élet minden területén használatos. Jelent anyagszerű tudást és elvonatkoztatott lényeget, dehumanizálódik, tárgyilagos és mennyiségi.	a) Elavult b) A világegyetem kategórizálása	a) Elavult b) Anyagszerű, kiváltságos formája a tudásnak
Reakció a modernizmusra XX. Sz. végétől napjainkig	Az emberi világban a jelentés is sokrétü. Az információ része a jelentés kialakításának vég nélküli folyamatában.	a) Része a társadalmi világ kialakulási folyamatának b) Elavult	a) A megismerés része b) Szerepet játszhat a tudás kialakításában, megszerzésében

1. táblázat, Az információtörténelmi modell, Arjan Vreeken (2005)[49] alapján, saját szerkesztés

A reprezentácionalista elveket valló John Locke (1632-1704) *Értekezés az emberi értelemről* (1690) című művében már tagadja az arisztoteliánus lélekfilozófiát és a platonikus ideatant. Locke szerint a dolgoknak ugyanis nincs belső formája. Művében megjelenik a tudás, a tapasztalat, amely szerint a tudás mindenkori tapasztaláson alapul, a tárgyakkal kapcsolatba kerülünk, azaz érzékeljük azokat, amely alapján érzékelhető tulajdonságokhoz juthatunk. Van egy másik forrása is tudásunknak, amikor az elme saját ideáival foglalkozik. Locke szerint az ideák észrevétele nem lényege, hanem művelete a léleknek. John Locke szerint az ideák a gondolkodás közvetlen tárgyai, az ideák nem maguk a fizikai tárgyak, hanem azok

[49] Vreeken, A., (2005). The History of Information: Lessons for Information Management, University of Amsterdam, Netherlands Sprouts: Working Papers on Information Systems, 5(2), fordította: Nádasi András, IKT Stratégia, Eger, 2013.

reprezentációi. Az ideák csak az elmében vagy az értelemben léteznek és a fizikai tárgyakat csak az ideák közvetítésével lehet megismerni.[50] [51] Állítása szerint, amit észlelünk, azok ideák és az ideák mentális jelleggel bírnak, feltételezi továbbá, hogy az ideák valamilyen értelemben tárgyi vonatkozásúak, materiálisak, illetve képzetek és nem ismeri el a tiszta intellektus létezését. Természetesen tovább lehet ezt a gondolatot folytatni, a „*cogito ergo sum*" azaz „*gondolkodom, tehát vagyok*" szállóige szerzőjének René Descartes (1596-1650) az értelem és az imagináció, az idea és a belső kép megkülönböztetésére szolgáló ezerszög ideájával. Az elmélet szerint az ezerszögről tudunk gondolkodni, a megvalósíthatóságának igazolásáról léteznek tudományos ismeretek, de magunk elé képzelni, mérnöki pontossággal már nehézkes. Gyakori eset, hogy egy szóban forgó nézet egy matematikaelméleti vonatkozással igazolható. Locke munkájában sokat foglalkozik nyelvészeti kérdésekkel is, miszerint jelentős a nyelv jelrendszer-jellege, a jel- és nyelvelmélet szoros kapcsolatban van egymással és a jelhasználat társadalmi és kulturális vonatkozásait nem lehet elhanyagolni. Locke talán ezekkel a gondolatokkal megfogalmazta a jel-, a kommunikáció- és az információtudomány alapelveit. Az „*information"* szó már megjelenik művében. A következő századok filozófusainak műveiben is találkozunk a jelekre, jelhasználatra vonatkozó gondolatokkal (Lambert, Kant, a francia felvilágosodás gondolkodói, Hegel).[52] Az újkorban az ókori és a középkori ideák elvesztették tekintélyüket, az információ az ideák, a világegyetemi eszmék felől az emberközpontúság felé, az emberi értelem és érzék felé irányult. Az empirista nézetek hamarosan újra felfedezték és ismét fontos szerepet töltött be az „*információ*", szemléltetve, hogyan írja le az érzékelés mechanikáját, a materiális anyagok hogyan alakítják (in-form) az érzékeket. Az információ fogalmában megtalálható az érzékek formálása, a világ az érzékek általi kifejezési módja. A fogalom környezete is megváltozott, az objektív, tárgyilagos formától eljutott az empirizmus szubjektív, érzéki megismeréséhez. Az újkor kezdetén az információ fogalma megszabadult metafizikai terhétől. [53] A jelentése megváltozott, immár nem az anyag formálását jelenti, hanem az érzékek tájékoztatását. Habár az érzékekre úgy tekintettek, mint egyfajta anyagra, egy alakított-formált anyagra, fontos megjegyezni, hogy az információ elvesztette a skolasztikából ismert ontologikus tulajdonságát. Ez a magas szintű lételméleti

[50] Forrai Gábor, A jelek tana: Locke ismeretelmélete és metafizikája, L'Harmattan, Budapest, 2005
[51] John Locke, (1779. körül) „*Az ideáknak és a szavaknak, mint a tudás hatalmas eszközeinek meggondolása tehát nem megvetendő része azok szemlélődéseinek, akik az emberi tudást egész terjedelmében kívánják áttekinteni. És ha mindezt pontosan mérlegelnénk, és kellően megfontolnánk, talán másféle logika és kritika származnék belőle, mint az, amelyet eddig ismerünk*."
[52] Fülöp Géza, Az információ, 2. bővített és átdolgozott kiadás, Budapest, 1996
[53] Nádasi András: Információtörténelem, „*Az információ, csakúgy, mint a kor egyetemes világnézete, az isteni rend által uralt világból lassan elmozdult az apró részecskék által mozgatott rendszerbe*." Eger, 2011.

jelentés ritkán fordult elő, csak az ismeretelméleti jelentés maradt meg.[54] Az információ elméleti megközelítése az ipari forradalom idején, végén ismét átalakult, megváltozott. A XIX század végén és a XX. század elején a bürokratikus államok kialakulásakor a lételméleti megközelítés elavult lett. Az információ ismét kapcsolódik a szerkezethez, az ipari forradalom központjában lévő gépekhez. Az információátadás lényege és összetétele letisztul nemcsak a szerkezetekben, de az elméleti kutatásokban is. Megjelenik a küldő és a befogadó fogalma, amely köré egy valós világ szerkezete kerül felépítésre. R.V. L. Hartley fogalmazta meg elsőként a (hír)közlési folyamat lényegét, amely szerint, az adó a rendelkezésére álló jelkészletből rendre jeleket választ ki, s azokból sorozatokat, "üzeneteket" állít össze (1927). Claude Elwood Shannon az információelmélet megalapítója, aki R.V. L. Hartley kérdésére, miszerint „hogyan lehetne mérni a távközlési rendszerekben továbbított információt?", adta meg a legáltalánosabb választ. Ahhoz, hogy mérni lehessen, le kell hámozni mindent, ami szubjektív, a jelentést s csak fizikai formáját kell vizsgálni (1948). Ezzel 1948-ra teszik az információtudomány kialakulását, a kibernetika és a matematikai információelmélet alapjainak megszületését is.[55] [56] Az „információ", évszázadokon keresztül nem volt definiálva, mindig új ismeretet, tudást jelentett, és aki birtokolta, az előnyt élvezett másokkal szemben, ezért a tudás hatalom is.[57]

2.3. AZ ADATVÉDELEM JELENTŐSÉGE, JOGTÖRTÉNETE ÉS HAZAI SZABÁLYOZÁSI RENDSZERE

2.3.1. AZ ADATVÉDELEM JELENTŐSÉGE ÉS JOGTÖRTÉNETE

Az információs rendszerek szempontjából vizsgált adatvédelmi szabályok tekintetében olyan tényezőket is figyelembe kell venni, amely nemcsak a szabályozási rendszer kialakítását, hanem a gyakorlati megvalósulását is figyelembe veszi. A történelem során az írás vagy írott jelek kialakulásával egy időben megjelent az információk, adatok védelmének igénye, ezért jelentős az adatvédelmi szabályok kialakulásának áttekintése és a kialakulására ható tényezők feltárása. A kutatásom során kizárólag a nyilvánossá tett joganyagokat, törvénycikkeket vizsgáltam, mivel a kutatás eredményeinek nyilvánossá tétele csak így garantálható. Természetesen létezhet olyan információ vagy adat, amely e fejezetben nem kerül megemlítésre

[54] Samuel Johnson (1709-1784), Angol szótár, 1755
[55] Fülöp Géza: Az információ, 2. bővített és átdolgozott kiadás, Budapest, 1996
[56] Király Zoltán: A magyarországi számítástechnika története az első elektromos számítógép megjelenéséig, Budapest, 2009.
[57] „*Scientia potentia est*." latin közmondás, Sir Francis Bacon természettudós lejegyzése alapján (1561-1626)

és mégis releváns lehet, de a terjedelem nem teszi lehetővé a teljes mértékű feltárást, inkább csak a szubjektív mintavételezésen alapuló kutatást és eredmények összegzését. Általános, hétköznapi szinten megfogalmazott vélemény, hogy az információvédelem vagy az adatvédelem, mint jogtényező a számítástechnika tömeges használatának elterjedésével és az adatrögzítés napi szintű gyakorlatával kezdett fejlődni és a két fogalom lényegében rendkívül hasonló. Kutatásaim bizonyítják, hogy ezen fogalmak már korábban léteztek, de a jogtényezők törvénybe iktatása, illetve használatának igénye csak a számítógépes adatrögzítés és -feldolgozás során került előtérbe. Az információ fogalmát az információelmélet következtében csak az elmúlt században határozták meg, amely szerint az adat meghatározása is ebbe a fogalomkörbe tartozik. Mindkét fogalom meghatározása az elmúlt egy században jelentős változáson esett át, leginkább bővült, mégis sokan úgy vélik az adatvédelem és az információvédelem az informatika tudományág körébe tartozik. A nézetek tisztázása e disszertációnak nem feladata, de néhány tényező útmutatóul szolgálhat a fogalmak értelmezéséhez. Az adatvédelemre és az információvédelemre irányuló szabályozás csíráit megtalálhatjuk már a korábbi joganyagokban is. Némi statisztikai kutatásom eredményeként megállapítottam, hogy az *adat* szó az elmúlt 1000 év, 1945-ig terjedő nyilvános jogi adattárban 10372 db jogszabályt és egyéb rendelkezést tekintve 80 joganyagot érint, míg az *információ* összesen csak egyet, az *adatvédelem*, mint jogtényező pedig nem található meg egyikben sem. Az *okirat* szó 313 joganyagban, a *titok* szó 58 joganyagban lelhető fel, ez utóbbi elsődlegesen katonai szabályozásban. Bár az *adatvédelem* nem található meg az ezeréves időszak nyilvános jogszabályai között, a jogtényezőhöz kapcsolódó szabályok, legfőképp a nyilvántartások kezelésére vonatkozó előírások és a szankciók annál inkább. A nyilvános joganyagokban megtalálható a hivatali titok illetéktelen, harmadik személyhez továbbításának vagy közzétételének vétsége, hamis tényekkel, okiratokkal való visszaélés bűntette és szankciója. Az 1946-tól napjainkig (a statisztikai adatok 2021. évi összegyűjtéséig) terjedő időszakban 6149 nyilvános és jelenleg hatályos joganyagban található az *adat* szó, 3276 joganyagban az *információ*, 866 joganyagban az *adatvédelem*, 11 joganyagban az *információvédelem*, 100 joganyagban az *adatbiztonság*, 103 joganyagban az *információbiztonság*, 1266 joganyagban a *titok*, míg az *okirat* 2279 joganyagban.[58] A találatok közül néhány érdekesebb rendelkezést célszerű külön is megemlíteni. A 1871. évi VIII. a bírák és bírósági hivatalnokok felelősségéről szóló törvénycikk szerint a bíró vagy bírósági hivatalnok az olyan tényeket vagy iratokat, amelyek esetében az információ csak hivatali állásánál fogva jut a tudomására vagy birtokába,

[58] Wolters Kluwer – Hungary, https://net.jogtar.hu/, statisztikai adatok összegyűjtése: 2021. március 20.

*hivatali titok*ként kell kezelni, és a hivatali titok közlése illetéktelen személlyel, bűntetendő. Az 1878. évi V., a magyar büntetőtörvénykönyv a bűntettekről és vétségekről szóló törvénycikk részletezi, illetve bűntettként rögzíti a titkos okirattal, az adattal vagy tudósítással, valamint hivatali irat tartalmával (hivatali titok) való visszaélést, az illetéktelen vagy harmadik személy („*A hivatali és ügyvédi büntettek és vétségek*" fejezete), ellenség („*A hűtlenség*" fejezete) részére nem megengedett, az állam vagy magánszemélyek kárára történő adatközlést. Ugyanezen törvénycikk „*A polgároknak választási joga ellen elkövetett büntettek és vétségek*" fejezetében a hamis adatbejegyzést, okirattal való visszaélést szintén bünteti. A hiteles adat, például az iparosok nyomtatványaikon vagy hirdetésein használt jelzők, jelvények vagy adat hiteles közléséről szóló szabályokat, különösen a 1884. évi XVII. ipartörvény törvénycikk, „*Az ipar gyakorlásáról*" című fejezete rögzíti. Ugyanezen törvénycikk rögzíti a lajstromba feljegyzendő személyes adatokat, úgymint az iparhatóság területén alkalmazott segédek és iparosok nevét, lakcímét, foglalkozását és munkaviszony adatait. Törvény által előírt személyes adatokra vonatkozó nyilvántartás szükségességét rögzíti a 1868. évi LIV. a polgári törvénykezési rendtartás tárgyában törvénycikk 202§, amely szerint, a nyilvántartás az adott perben megnevezett és meghallgatott tanuk adatait, úgymint vezeték- és keresztnevét, életkorát, vallását és foglalkozását tartalmazza. A hivatkozott két törvénycikk alapján kötelezően rögzített nyilvántartások személyes adatokat tartalmaznak, amelyek az adott irat, illetve a hivatali eljárás részét képezi, így hivatali titok alá esik, kivéve, ha arról valamely jogszabály vagy egyéb előírás másképp nem rendelkezik. Ebben a tekintetben, lényegében az adatkezelés és az adatvédelem mai gyakorlatnak csírájával találkozhatunk. Mai meghatározás szerint az adatvédelem a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége[59]. Bár úgy tűnik, hogy 1945. előtt a hivatali ügyek gyakorlásában az iratok és a benne szereplő adatok, így a személyes adatok védelme fontos szerepet kapott, mégis az adatvédelem, mint jogtényező deklarálására csak jóval később került sor. Az Európai Unió alapját képező értékrendek közé tartozik az uniós polgárok alapvető személyes jogai is. Európa elmúlt néhány évszázad történelmének meghatározó elemei az alapvető jogok megerősítésére irányuló törekvések, az emberi és polgári jogokról szóló nyilatkozatok 18. századi kihirdetése és az európai civilizált államok alkotmányos rendjének, emberi jogi intézményrendszerének megszilárdítása. Az Európa Tanács keretein belül számos egyezmény született a gazdaság, a kultúra, a szociálpolitika és a

[59] Nemzeti Adatvédelmi és Információszabadság Hatóság, https://naih.hu/adatvedelmi-szotar, letöltés: 2021. március 20.

jog területén, így a számunkra jelentős területen, az emberi jogok védelmére irányuló jogvédelmi rendszer megalapozására és kialakítására vonatkozóan. Az egyik legjelentősebb és egyben legismertebb európai egyezmény az 1950. november 4-i római Egyezmény az emberi jogok és alapvető szabadságok védelméről (EJEE)[60] [61]. Az emberi jogok intézményének fontosságát hangsúlyozva az Egyezményhez az Európa Tanács minden tagja csatlakozott. Az egyezmény egyedülálló módon jogi és gyakorlati szempontból is jelentős, bár alapkövetelményeket határozott meg az európai tagállamok számára az emberi jogok megóvása, így például a magán- és családi élet tiszteletben tartása érdekében, ugyanakkor lényegét tekintve jogvédelmi rendszert is megalapozott, amely lehetővé tette a strasbourgi intézmény, az Európai Emberi Jogi Bizottság és az Európai Emberi Jogi Bíróság számára, hogy az európai emberi jogi visszaélésekről döntsenek. Az intézményhez később más szervezet is kapcsolódott, 1994-ben az Európai Biztonsági és Együttműködési Szervezet (EBESZ), amelynek célja különösen az európai államok közötti biztonsági háló megteremtése, amely a konfliktusok békés eszközökkel való elsimítását támogatja. 1980-ban a számítástechnika a mai fejlettséghez viszonyítva még gyerekcipőben járt, mégis a „*háborítatlansághoz való jog*”[62] meghatározása után közel száz évvel később előtérbe került az adatalanyok védelme, az emberi méltóság, ami sérthetetlen és korlátozhatatlan[63], tehát a magánélet védelme és a személyes adatok határokon átívelő áramlásának szabályozási igénye. Az információs technológia fejlődése és az elektronikus adatfeldolgozás felgyorsította a személyes adatok kezelésére vonatkozó szabályozási törekvéseket, ami 1980-ban a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Irányelveinek kiadásához vezetett[64] [65]. Az irányelvek meghatározásai között megtalálhatjuk a mai használatban lévő alapfogalmakat, úgymint az adatellenőrző[66], a személyes adat[67], vagy a személyes adat határokon átívelő áramlása[68]. A felsorolt alapfogalmak

[60] Egyezmény az emberi jogok és alapvető szabadságok védelméről, Róma, 1950. november 4., 8. CIKK „Magán- és családi élet tiszteletben tartásához való jog, 1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák.” https://www.echr.coe.int/documents/convention_hun.pdf letöltés: 2021. március 27.

[61] 1993. évi XXXI. törvény, az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről

[62] Nemzeti Adatvédelmi és Információszabadság Hatóság, Szemelvények az információs jogok felügyeletének elmúlt 25 évéből, szerk: Dr. Péterfalvi Attila

[63] Péterfalvi Attila, A magyar adatvédelmi jogi szabályozás változásai, in: Állam és Jog – Kodifikációs kihívások napjainkban, Magyar Jog- és Államtudományi Társaság – Gondolat, Szeged-Budapest, 2013

[64]Gazdasági Együttműködési és Fejlesztési Szervezet, OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról, 1980., Áttekintés 2003. http://www.oecd.org/sti/ieconomy/15590228.pdf, letöltés: 2021. március 21.

[65] Péterfalvi Attila, Átláthatóság a védelmi igazgatásban, Budapest, 2014.

[66] az, aki kompetens dönteni a személyes adatok tartalmáról és felhasználásáról

[67] lényegét tekintve bármely információ, ami egy meghatározott, azonosítható személyre vonatkozik

[68] a nemzeti határok közötti mozgó személyes adatok

meghatározása mérföldkő az adatvédelem szabályozása terén, mivel személyes adat lehet egy olyan azonosító karaktersorozat is, amely egy azon személyt meghatároz, így a személyi szám, a személyi igazolvány száma, az adóazonosító jel vagy a TAJ. Adott karaktersorozat felhasználásával egy információs rendszerben nemcsak az adott személy adataihoz férhetünk hozzá, úgymint születési adatok, lakcím, anyja neve, hanem a szakrendszer típusától függően a személy bérjegyzék adataihoz, bankszámla egyenlegéhez is. Az Internet adta lehetőségekkel a személyes adatok is utaznak egyik országból a másikba, anélkül, hogy egyes esetekben tudomást szereznénk róla. Ilyen adatmozgási lehetőséget biztosít a közösségi média vagy egy online újság, amely felületén megjelenő publikussá tett adat, mint például egy személyről készített és megosztott fénykép, név vagy más személyes adat, ugyanúgy megjelenhet az Egyesült Államokban, Japánban vagy Ausztráliában. Az Irányelvben rögzítésre kerültek a nemzeti alkalmazás alapelvei is, amelyek a jelenlegi nemzeti jogszabályokban is megtalálhatóak, úgymint a korlátozott adatgyűjtés[69], az adatminőség[70], a szándékmegjelölés[71], a felhasználási korlátozás[72], a *biztonsági garancia*[73]. Az Irányelv ezen alapelvének vonatkozásában lényegében az adatvédelem és informatikai biztonság szabályozása találkozik, ezért a biztonsági garancia elkülöníthető a többi alapelvtől, mivel az információbiztonsági alapelvek[74] részét képezi. Az OECD információs rendszerek biztonságára vonatkozó irányelve szerint a biztonságot olyan mértékben kell megvalósítani, hogy teljesíthesse az információ szabad áramlásának, az információ és kommunikáció titkosságának, a személyes adatok megfelelő védelmének, a nyitottság és az átláthatóság elvét.[75] Tehát az adatvédelem és az információbiztonság szabályozása szorosan kapcsolódik egymáshoz, és egy személyes adatokat nyilvántartó információs rendszer tekintetében mindkét típusú szabályozást figyelembe kell venni és a rendelkezéseket be kell tartani. A további, az Irányelvben rögzített alapelv a nyitottság, az egyéni részvétel és a felelősségre vonás, amelyek a nyitottsági politika

[69] a meghatározás alapján személyes adatot gyűjteni csak a *törvényesség* és *tisztesség elve* szerint lehetséges, az érintett személy tudtával és beleegyezésével

[70] az adatokat a relevancia, a *szükségesség*, a *pontosság*, a *teljesség* és az *aktualitás elve* alapján lehet kezelni

[71] már az adatgyűjtés kezdetén meg kell határozni és később az adatokat csak a megjelölt célokra lehet felhasználni, a *célhoz kötöttség elve* szerint

[72] a személyes adatokat nyilvánosságra hozni, rendelkezésre bocsátani vagy bármilyen más módon felhasználni a rendelkezésben meghatározott célokon kívül nem lehet, kivéve, ha az adatalany vagy törvény ettől eltérően nem rendelkezik

[73] a személyes adatokat nyilvánosságra hozni, rendelkezésre bocsátani vagy bármilyen más módon felhasználni a rendelkezésben meghatározott célokon kívül nem lehet, kivéve, ha az adatalany vagy törvény ettől eltérően nem rendelkezi

[74] ISO/IEC 27000 szabványcsalád - Információbiztonsági Irányítási Rendszer

[75] Gazdasági Együttműködési és Fejlesztési Szervezet, Az információs rendszerek és hálózatok biztonságára vonatkozó OECD irányelvek: Útban a biztonságkultúra felé, 1992. https://www.oecd.org/sti/ieconomy/15582292.pdf Áttekintés, 2003.

folytatását, az egyén igazolás kérésének, betekintési, adattörlési, -helyesbítési, -kiegészítési és -módosíttatási jogának gyakorlását, valamint az adatellenőrző felelősségre vonhatóságának lehetőségét támogatja. Bár az 1959. évi IV. első Polgári Törvénykönyvben deklarálásra kerültek a *személyhez fűződő jogok*, így a névjog, a jóhírnévhez való jog, a levéltitokhoz való jog, a magánlakáshoz fűződő jogok, valamint a képmáshoz és hangfelvételhez való jog is, de a komplex adatvédelmi szabályok megfogalmazása és gyakorlata még váratott magára. Az OECD Irányelvek alapelveinek magyarországi alkalmazása a 15/1991. (IV. 13.) AB határozat megalkotásával került előtérbe, amelyben már szerepel a célhoz kötöttség, a magántitok és a személyes adatok védelméhez való jog, továbbá az információs önrendelkezési jog, az érintett beleegyezése, az adatfeldolgozás útja, valamint az adatok felhasználásának módja. A határozatban foglaltak által az „Alkotmány 59. § (1) bekezdése szerint a Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog”[76]. A határozat rendelkezései garanciát nyújtanak a személyhez fűződő jogok érvényesítéséhez, úgymint az adattovábbítás vagy az adatok nyilvánosságra hozásának korlátozása, továbbá megállapításra került a harmadik személy, az adatfeldolgozó, az adattovábbítás, a nyilvántartott adatok köre, valamint az anonim adatok fogalma is. Újabb mérföldkövet jelentett a 1992. évi LXIII. törvény, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Avtv.). A törvényben megfogalmazásra kerültek az adatkategóriák, tehát a személyes adat[77], a különleges adat, a közérdekű adat, továbbá az adatkezelés[78], az adattovábbítás, a nyilvánosságra hozatal, az adatkezelő, az adattörlés[79]. A törvény fokozatos fejlődésen ment keresztül igazodva az európai egyezményhez és az irányelvekhez, így elsődlegesen az Európa Tanács 1981. január 28-i 108. számú, az egyéneknek a személyes adataik gépi feldolgozása során való védelméről szóló egyezményhez, valamint az 1995. évi 95/46/EK Európa parlamenti és tanácsi irányelvéhez. Az egyezmény volt az adatvédelem területén elfogadott, első jogilag kötelező erejű nemzetközi okmány, aminek célja, hogy minden egyén számára biztosítsa a magánélethez való jogait és az alapvető szabadságjogokat, egyben ezeket a jogokat tartsák tiszteletben a személyes adatok gépi feldolgozása során. A 108. számú egyezményt azért alkották meg, hogy védelmet nyújtson

[76] 15/1991. (IV. 13.) AB határozat
[77] Az Avtv. meghatározása szerint: „*a meghatározott természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés.*”
[78] Az Avtv. meghatározása szerint: „*az alkalmazott eljárástól függetlenül a személyes adatok felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt), adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is*.”
[79] Az Avtv. meghatározása szerint: „az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk nem lehetséges.”

különösen a személyes adatok gyűjtésével és feldolgozásával kapcsolatos visszaélések ellen, és egyúttal támogassa a határokon átnyúló személyes adatok áramlásának szabályozását. Az egyezményben meghatározott elvek alapján az adatokat csak tisztességesen és törvényesen szabad gyűjteni és feldolgozni, csak meghatározott és törvényes célra szabad tárolni, továbbá csak a tárolás céljához szükséges ideig szabad tárolni. Az egyezmény érinti az adatok minőségét, relevanciáját, és a feldolgozás célját vagy az arányosság, továbbá a pontosság elvét. Az 1995. évi irányelv megfogalmazta az adatfeldolgozó rendszerek polgárok szolgálatának célját, és célkitűzése többek között a személyek alapvető jogainak és szabadságainak tiszteletben tartása, különösen a magánélethez való jog tiszteletben tartása. Az informatikai rendszerek használatával előtérbe került a személyes adatok feldolgozása, cseréje, a személyes adatok határokon keresztüli áramlásának lényeges megnövekedése.[80] Az irányelv előtérbe helyezte a növekvő tudományos és műszaki együttműködésnek köszönhetően az új telekommunikációs hálózatok összehangolt használatát, amely során elengedhetetlen az adatcsere, és ami megkönnyíti a személyes adatok határokon keresztül történő áramlását. Az irányelv előírta, hogy tagállamoknak többek között meg kell határozniuk, hogy a személyes adatok feldolgozása milyen feltételek mellett lehet jogszerű, továbbá az adatok minőségét érintő elveket, úgymint törvényesség, garancia, relevancia, pontosság, vagy az adatfeldolgozás jogszerűségére vonatkozó kritériumokat, úgymint az érintett egyértelmű hozzájárulása, szerződés vagy jogi kötelezettség teljesítése, közérdekből elvégzendő feladat köre, illetve az érintett tájékoztatására, tiltakozására, titkosságra és biztonságra vonatkozó előírásokat. A hazai jogalkotók az Avtv. szabályainak törvénybe iktatásakor figyelembe vették az európai egyezményt. Bár 1992-ben a lakosság még nem használta napi szinten az informatikai eszközöket, sőt az informatikai képzés csak bevezető szakaszban járt, ennek ellenére az adatvédelmi törvényünk az általános, elektronikus adatkezelésre is vonatkoztatható előírásaival útmutatóul szolgált a későbbi informatikai adatkezelést alkalmazók számára. A középiskolai képzésben már megjelent a BASIC programozási nyelv, mint tananyag, valamint a felhasználói ismeretek, mégpedig a szövegszerkesztés, az adatbáziskezelés, a táblázatkészítés és -kezelés, a modellezés, a szimuláció és folyamatirányítás, a robotika vagy a programozás alapjai. A technikai fejlődés és az oktatási igények, valamint az adatvédelmi előírások törvényi szintre emelése hatással voltak a mindennapi életre és társadalmi, kulturális befolyással bírt. Az Avtv.

[80] AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA, Az Európai Parlament és a Tanács 95/46/EK irányelve, (1995. október 24.), a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A31995L0046

adatvédelmi rendelkezései nemcsak a papír alapú adatokra, hanem az elektronikus módon tárolt adatokra is vonatkozott, annak ellenére, hogy az 1992. évben elfogadott Avtv. jogszabályban még sem az *informatika* vagy a *számítástechnika*, sem pedig az *elektronikus* szó nem szerepelt. Az *informatika*[81] és a *számítástechnika*[82] 2004. január 1-től hatályos Avtv. *Adatbiztonság*, illetve *Automatizált egyedi döntés* részében, míg az utóbbi a 2005. évi módosítás során került rögzítése *A közérdekű adatok nyilvánossága* című fejezetben. Hazánk egyedülálló módon rögzítette az adatvédelemre és az információszabadságra vonatkozó rendelkezéseit egy ugyanazon törvényben[83], ezen kívül az adatbiztonság egyes előírásait is tartalmazza. Az Avtv. rendelkezései folyamatosan bővültek, amely során figyelembe vették az 1995. évi irányelvet, így például az adatkezelő és adatfeldolgozó egymástól megkülönböztetett, jogszabály szintű deklarálására 1999-ben került sor, ami által egyértelműbbé vált a két jogtényező közöti jelentős különbség. Az Adatvédelmi törvényre a 2011. évi jelentősebb módosításáig és az Infotv. hatályba lépéséig a finomhangolás időszaka a jellemző. Alkalmazták és törvénybe iktatták az irányelv adatkezelésre[84] irányuló szabályát, továbbá az érintett személyt megilleti a tiltakozás joga, kifogásolhatja az adatainak kezelését, valamint kérheti a megszüntetését vagy a törlését. 2004-től az értelmező rendelkezések meghatározásait pontosították és új értelmezéseket is rögzítettek, különösen a személyes adat, különleges adat, bűnügyi személyes adat, hozzájárulás, tiltakozás, adattovábbítás, -törlés, -zárolás vagy –megsemmisítés, illetve személyesadat-nyilvántartó rendszer, adatállomány, harmadik személy és harmadik ország meghatározását. 2005-ben a törvényben pontosításra került a közérdekű adat definíciója is. A személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való alkotmányos jog védelmét az új Alaptörvény[85], valamint a 2011. évi CXII. Infotv. megalkotásáig szakombudsman, mint adatvédelmi biztos[86] látta el. Az Infotv. új alapokra helyezett komplex, immár nem csupán adatvédelmi törvény, hanem információs önrendelkezési jogról és az információszabadságról

[81] Avtv. 2004. január 1-től hatályos rendelkezése szerint: „*Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.*"

[82] Avtv. 2004. január 1-től hatályos rendelkezése szerint: „*Kizárólag számítástechnikai eszközzel végrehajtott automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésére csak akkor kerülhet sor, ha ahhoz kifejezetten hozzájárult, vagy azt törvény lehetővé teszi. Az érintettnek álláspontja kifejtésére lehetőséget kell biztosítani.*"

[83] Nemzeti Adatvédelmi és Információszabadság Hatóság, Szemelvények az információs jogok felügyeletének elmúlt 25 évéből, szerk: Dr. Péterfalvi Attila

[84] csak az adatalany önkéntes, határozott és tájékozott beleegyezésen alapuló hozzájárulása alapján történhet

[85] Magyarország Alaptörvénye (2011. április 25.), hatályos: 2012. január 1.

[86] Avtv. rendelkezése szerint: „*A személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való alkotmányos jog védelme érdekében az Országgyűlés adatvédelmi biztost választ*"

szóló rendelkezés, ami első ránézésre is azt sugallja, hogy túlmutat az adat fogalmán, és az információ teljes fogalomtárával rendelkezik. A jogalkotó új elemként rögzítette az érintett, mint bármely információ alapján azonosított vagy azonosítható természetes személy fogalmát és ennek megfelelően módosította a személyes adat meghatározását is[87]. Az Infotv. nagyobb hangsúlyt ad az előzetes tájékoztatási kötelezettségnek, melynek lényege, hogy az érintettet előzetesen tájékoztatni kell, az adatkezelés tényéről, módjáról, ami hozzájáruláson alapul vagy kötelező jellegű. Az érintettet továbbá részletesen tájékoztatni kell az adatainak kezeléséről, illetve az adatkezelés céljáról, jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosultak köréről, az adatkezelés időtartamáról, valamint az adatokhoz való hozzáférők személyéről (amennyiben például az adatfeldolgozó harmadik személy). Az Infotv. rendelkezései szerint tájékoztatni kell az érintettet adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, vagy adatfeldolgozó szervezeteknél, továbbá a pénzügyi szervezeteknél, az elektronikus hírközlési és közüzemi szolgáltatónál belső adatvédelmi felelőst kell alkalmazni, aki jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkezik. A belső adatvédelmi felelős, mint a személyes adatkezelés és adatfeldolgozás őre, aki közreműködik és segíti az adatkezeléssel összefüggő döntések meghozatalát, és az érintettek jogainak biztosítását, ellenőrzi a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek való megfelelést, kivizsgálja a bejelentéseket, tájékoztatja az adatkezelőt vagy az adatfeldolgozót az esetlegesen észlelt jogosulatlan adatkezelésről és felhívja a figyelmet annak megszüntetésére, gondozza az intézményi adatvédelmi és adatbiztonsági szabályzatot, vezeti a belső adatvédelmi nyilvántartást, illetve koordinálja az adatvédelmi oktatást. Lényeges változást hozott az Infotv. történetében a GDPR jogharmonizáció. Az Infotv. rendelkezése értelmében kategorizálhatók a személyes adatok[88], így személyes adatnak minősül az érintettre vonatkozó a vezetéknév és

[87] 1992. évi személyes adat meghatározása (közlöny állapot): „*a meghatározott természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés*."
2011. évi személyes adat meghatározása (közlöny állapot): „*az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés*;"
[88] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.), „*Személyes adatnak minősül az azonosított vagy azonosítható érintett személlyel kapcsolatos bármely információ*."
AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR),
4. cikk (1) bek. szerint „„*személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható*"

keresztnév, a lakcím, a személyazonosító igazolvány, illetve útlevél száma, személyi szám, adóazonosító, TAJ, az SZJA-val kapcsolatos információk, az oktatási azonosító szám, így a diákigazolvány száma vagy a tanulmányi információs rendszerben használt azonosító, a kulturális azonossággal kapcsolatos információk, a számítógép azonosító száma (MAC), a hasznát internet protokoll (IPv4, IPv6) címe, email cím, az egészségügyi célból gyűjtött adatok, amelyek egyértelműen beazonosítják az érintettet. További, speciális, személyes adatkategóriák a különleges adatok[89], amelyek lehetnek faji, etnikai származásra, politikai nézetre, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra vonatkozó adatok, genetikai, biometrikus vagy egészségügyi adatok, bűnügyi személyes adat, egy adott bűnüggyel bármely módon kapcsolatba hozható személyes adat, szexuális irányultságra vonatkozó adatok. A személyes adatok kategóriái tovább bonthatók, ami függ az adott információs rendszer típusától, a szakrendszertől, az alkalmazott adatbázisrendszerben felépített struktúrától és az információs rendszerben kialakított adatcsoportoktól. A szakrendszer típusának megfelelően kialakíthatók, az érintetthez közvetlenül összefüggésbe hozható személyes adatok, mint a születési adatok, valamint a további adatok a lakóhelyre vonatkozóan, a munkavállalói, a személyi jövedelem adóhoz kapcsolódó jövedelem és adójárulék vagy a nyugdíj megállapításhoz szükséges adatok. Információs rendszerben kategorizálható további adatcsoportok az egészségügyi, a tanulmányi, az önkormányzati (helyi adózás nyilvántartásai) adatok, az internethasználat, a telefonhasználat, vagy a szórakozási tevékenység (éttermi, szállodai, utazási irodai) közlekedés információi. A természetes személyek személyes adatainak kezelése védelmének érdekében és az adatok szabad áramlásáról szóló rendelkezések szerint egy vállalkozás, szervezet vagy intézmény akkor gyűjtheti és használhatja fel a személyes adatokat, ha szerződést kötött az érintettel[90], jogi kötelezettségének, úgymint adó- és járulékfizetés, eleget tesz eleget[91], a személyes adatok kezelése az érintett érdekeit szolgálja[92], a közérdekű feladatok, közintézmények feladatainak törvény által előírt ellátásához szükséges, vagy az adatkezelő jogos érdekeinek érvényesítéséhez szükséges[93]. Az előbbiektől eltérő esetekben a vállalatnak, szervezetnek vagy intézménynek a természetes személy előzetes hozzájárulását kell kérnie a

[89] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.),
„5§ (2) *Különleges adat b) akkor kezelhető, ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli.*"
[90] különösen áru vagy szolgáltatás igénybe vételéről, vagy a munkavégzésre utaló jogviszony létesítéséről
[91] ha az adatkezelés alapja jogi előírás
[92] elsősorban, ha a személyét érintő védelem vagy a személyes adatvédelem okán elengedhetetlen az adatkezelés
[93] például banki szolgáltatás igénybevétele esetén

személyes adatainak gyűjtéséhez vagy annak ismételt felhasználásához és a hozzájárulásnak egyértelműnek kell lenni, megtörténtét egyértelműen lehessen igazolni. A hozzájárulás elektronikus úton is engedélyezhető, ha a hozzájárulást adó személy egyértelműen azonosítható. Világos és közérthető módon tájékoztatni kell az érintett személyt a tárolandó információk okáról, típusáról, a tárolás időintervallumáról, valamint az érintettet megillető adatvédelmi jogokról[94], adatkezelőre és az adatvédelmi tisztviselő (amennyiben van) elérhetőségére, továbbá az esetlegesen alkalmazott adatfeldolgozóra, illetve adattovábbításra vonatkozó információkról. Az Infotv. és az uniós adatvédelmi szabályok értelmében a személyes adatok kezelése tisztesség és szabályszerűség elve alapján, meghatározott és jogszerű cél érdekében történhet, ezen kívül nem haladhatja meg a szükséges mértéket (adattakarékosság elve). Személyes adatkezelés az érintett személy hozzájárulásával, a szerződéses kötelezettség teljesítése érdekében, a jogi kötelezettség teljesítése érdekében, az érintett létfontosságú érdekeinek védelmében, a közérdekből elvégzendő feladat végrehajtása érdekében lehetséges, valamint a szervezet jogos érdekeit szolgálja. Kiskorúak tekintetében, olyan személyek, akik szintén igénybe veszik az árukat és szolgáltatásokat, a való életben és a virtuális térben egyaránt. Ahhoz, hogy online szolgáltatásokat vehessenek igénybe, úgymint közösségi oldalakat látogathassanak, zenét vagy játékot tölthessenek le applikáción keresztül, sokszor a szülők jóváhagyására lenne szükség. A szolgáltatásokhoz meg kell adni a gyermek személyes adatait, aminek engedélye kiskorú személy esetében a szülőre illetve gondviselőre hárul. A 16. életévüket betöltött fiatal esetében szülői hozzájárulás nem szükséges. A 16. év alatti kiskorú esetében pedig gyakorlatilag nehezen megoldható a szülői hozzájárulás, ha a gyermek saját informatikai eszközére, így telefonjára, vagy laptopjára tölti le az alkalmazást. Ugyanakkor fontos lenne, hogy hatékonyan ellenőrizni lehessen a valós szülői hozzájárulást. A kétfaktoros azonosítási módszer lehetőséget nyújt ennek kiküszöbölésére, de jelenleg legfőképp kormányzati és pénzintézetek alkalmazzák ezeket a szigorúbb ellenőrzési módszereket. Általában elfogadott, hogy a kormányzati (beleértve a helyi önkormányzati vagy a közigazgatási, adó és egészségügyi vagy oktatási) és banki ügyek intézéséhez szigorúbb azonosítási módszer tartozik, de ugyanígy a szórakozáshoz, így például a filmnézéshez, közösségi oldalak használatához ez a módszer már nehezebben alkalmazható. A szórakoztatóipar vagy a kereskedelem a kapott személyes adatokat profilalkotásra, direkt marketing tevékenységre is felhasználja, amitől sok felhasználó idegenkedik és kifejezetten

[94] úgymint az adatokhoz való hozzáférés, helyesbítés, törlés, panasztétel vagy tiltakozás, az adatok kezeléséhez való hozzájárulás visszavonása

zavaró tényezőként tekintenek például a beazonosított IP cím, operációs rendszer és böngészői adatok alapján kapott kereskedelmi ajánlatokra. A GDPR adatvédelmi szabályozásnak köszönhetően az adott weboldalt látogatót tájékoztatják adata tárolásáról, valamint a nyomkövetés módszeréről, és a felhasználó dönthet annak elfogadásáról vagy tiltásáról. A cookie-k vagy sütik, kisméretű szöveges információkat tartalmazó fájlok, melyeket a felkeresett weboldalak helyeznek el a felhasználók informatikai eszközén vagy mobilkészülékén. A GDPR rendelkezéseinek köszönhetően ez a tevékenység csak a felhasználó előzetes hozzájárulásával lehetséges. A sütiket annak érdekében használják, hogy a felhasználói beállítások elmentésével javítsák a felhasználói élményt, a weboldalak működését, gyorsabb hozzáférését és hatékonyságát. A sütik nyomon követik a felhasználó internetes aktivitását és felhasználói profilkészítésre[95] alkalmas, valamint hatékonyan támogatja a direktmarketing tevékenységet. Amennyiben a látogatott weboldalak egészségügyi témájúak, úgy a felhasználó egészségügyi állapotára vonatkozó digitális profil alakítható ki. Ezen profil kialakítására irányuló adatgyűjtést a weboldal felhasználója megtilthatja vagy korlátozhatja. A GDPR szabályainak alkalmazásával mindez kezelhetőbbé vált az Európai Unióban és Magyarországon egyaránt. A profilalkotás bűnmegelőzésre, vagy -üldözésre hatékonyan felhasználható. A mesterséges intelligencia technológiai fejlődésével az automatizált döntéshozatal és profilalkotás is egyre előtérbe kerül. Az adatkezelés az automatizált adatkezelést és döntéshozatalt is érinti, mivel az érintettnek jogában áll, hogy kifejezhesse kérését a tekintetben, hogy ne születhessen személyükkel kapcsolatos olyan döntés, amelynek alapja kizárólag az automatizált adatkezelés. Természetesen létezik néhány kivétel, így az érintett hozzájárulásán alapuló automatizált döntéshozatal. Jogi előíráson alapuló automatizált döntéshozatal esetében tájékoztatnia kell az érintettet az automatizált döntéshozatal tényéről, az érintett élhet az emberi döntésen alapuló felülvizsgálat jogával, illetve az érintett élhet az automatizált döntés ellen irányuló tiltakozás jogával. Amennyiben az adatkezelés mégsem lenne jogszerű és az érintett által a szolgáltatónak eljutatott kérés és felszólítás hasztalan, valamint kizárólag jogérvényesítés útján rendezhető az adatvédelmi jog megsértése, az Infotv. lehetőséget nyújt arra, hogy az érinett panasztétel gyakorlásával és kivizsgálásra irányuló kéréssel közvetlenül a Nemzeti Adatvédelmi és

[95] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)
„„*profilalkotás": személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják*;"

Információszabadság Hatósághoz (NAIH, Hatóság) fordulhat, vagy lehetősége van közvetlenül a bíróságon érvényesíteni a keresetet. Amennyiben a Hatóság megállapítja a kérés jogszerűségét, illetve a károkozás tényét, úgy az érintett kártérítésre is jogosult lehet, tehát az Infotv. rendelkezéseinek be nem tartása szankcionálható. Személyes adatok nyilvántartása esetében adatvédelmi hatásvizsgálatot[96] minden esetben célszerű elkészíteni, különösen akkor, ha az adatkezelés magas kockázattal járna a nyilvántartott személyek jogaira és szabadságaira nézve. Az adatvédelmi hatásvizsgálat rámutathat az esetleges magas kockázattal járó adatkezelésre, illetve ennek elkerülése céljából meghozott, szükséges intézkedések megvalósítására. Amennyiben a végrehajtott intézkedések, úgymint például technológiai fejlesztés, struktúraváltás, felhasználói tudatosítás által a kockázatok csökkenthetők, és az adatkezelés már alacsonyabb kockázattal járna, úgy az adatkezelés és a feldolgozás művelete javasolható. A hatásvizsgálatot célszerű elvégezni a nyilvántartás készítését megelőzően, így eredménye befolyásoló tényező lehet különösen a nyilvántartás szükségszerűségére és az adattakarékosság elvére vonatkozóan. Az adatkezelő felel az adatvédelmi kockázat forrását, jellegét, egyediségét és súlyosságát felmérő hatásvizsgálat elvégzéséért.[97] Adatvédelmi hatásvizsgálatot kell végezni abban az esetben, ha a személyes adatkezelés célja, hogy a természetes személyekkel kapcsolatban döntést lehessen hozni[98], vagy ha cél a nyilvános helyek nagymértékű megfigyelése, és amennyiben a megfigyelést elektronikus optikai eszközök alkalmazásával hajtják végre, illetve ha az illetékes felügyeleti hatóság állásfoglalása szerint az adatkezelés valószínűsíthetően magas kockázattal járna az érintettek jogaira és

[96] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR),
(90) „*A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó ilyen esetekben az adatkezelő – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérje a magas kockázat különös valószínűségét és súlyosságát – az adatkezelés előtt adatvédelmi hatásvizsgálatot végez. Ez a hatásvizsgálat magában foglalja különösen az említett kockázat mérséklését, a személyes adatok védelmét, valamint az e rendeletnek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat.*"

[97] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR),
(90),„*Ez különösen vonatkozik egyrészt azokra a nagymértékű adatkezelési műveletekre, amelyek jelentős mennyiségű személyes adat regionális, nemzeti vagy szupranacionális szintű kezelését célozzák, és amelyek az érintettek jelentős számára hatással lehet, és amelyek például az adatok érzékenysége folytán valószínűsíthetően magas kockázattal járnak, másrészt azokra az adatkezelési műveletekre, amelyeknél nagy arányban a technológia elismert állásának megfelelő új technológiát alkalmaznak, valamint olyan más adatkezelési műveletekre is, amelyek magas kockázattal járnak az érintettek jogaira és szabadságaira nézve, különösen, ha az említett műveletek megnehezítik az érintettek számára, hogy a jogaikat gyakorolják*."

[98] profilalkotás alapján elvégzik a természetes személyek személyes jellemzőinek szisztematikus és kiterjedt értékelését, a személyes adatok különleges kategóriáira, a biometrikus adatokra vagy a büntetőjogi felelősség megállapítására és a bűncselekményekre vagy a kapcsolódó biztonsági intézkedésekre vonatkozó adatok kezelését követően.

szabadságaira nézve. A hatásvizsgálat lefolytatása nem kötelező abban az esetben, ha a személyes adatok kezelése nem tekinthető nagymértékűnek, vagy ha az adatkezelést végző szakorvos, illetve egészségügyi szakember betegeinek, illetve az ügyvéd ügyfeleinek személyes adatára vonatkozik. Az adatkezelőnek konzultálnia kell a Nemzeti Adatvédelmi és Információszabadság Hatósággal (NAIH) abban az esetben, ha az adatvédelmi hatásvizsgálat szerint az adatkezelési műveletek olyan magas kockázattal járna, amelyet az adatkezelő nem képes csökkenteni a rendelkezésre álló erőforrásokkal, különösen a technológiai intézkedésekkel. A hatásvizsgálat kiterjedhet az alábbi tényezőkre, úgymint az adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára, az érintett jogait és szabadságait érintő kockázatok vizsgálatára, a kockázatok kezelésétre irányuló intézkedések bemutatására[99]. A hatásvizsgálat lefolytatásánál, az adatkezelői és adatfeldolgozói feladatok ellátásánál a vonatkozó magatartási kódex előírásait figyelembe kell venni. A magatartási kódex kialakítására kötelező érvényű rendelkezés egyelőre nem létezik, de az ajánlások és a GDPR elvek alapján néhány etikai szabály megállapítható. A magatartási kódex alapvető célja, hogy biztosítsa különösen a tisztességes és az átlátható adatgyűjtést, adatkezelést, a nyilvánosságot és az érintettek tájékoztatását, és jogainak gyakorlását, az adatkezelők jogos érdekeit meghatározott körülmények között, a személyes adatok anonimizálását, valamint a 24. és a 25. cikkben részletezett, valamint a 32. cikkben említett adatkezelés biztonságát szolgáló intézkedéseket és előírásokat.

2.3.2. ADATVÉDELMI SZABÁLYOZÁS JÖVŐJE – EURÓPAI ADATVÉDELMI REFORM

Az európai Általános adatvédelmi rendelet (GDPR) mellett két adatvédelmi reformmal találkozhatunk, a bűnügyi irányelvvel és az e-privacy rendelettel. A 2016/680/EU bűnügyi irányelvet[100] a 2016/679/EU GDPR rendelet mellett az Európai Parlament és a Tanács 2016. április 27-én fogadta el, ami a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv. Az irányelv nemzeti jogszabályba való átültetését a tagállamoknak 2018. május 6-ig

[99] különösen a személyes adatok védelmét, az érintettek és más személyek jogait és az érintettek jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és technológiákat.
[100] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/680 IRÁNYELVE (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről

kellett megvalósítani. Az irányelv célja a 95/46/EK adatvédelmi irányelv és a szóló 2008/977/IB tanácsi kerethatározatban[101] meghatározott szabályok modernizálása, továbbá a polgárok alapvető jogainak és szabadságainak védelme, a természetes személyek adatainak védelmére az illetékes hatóságok által, úgymint a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása során. Az irányelv további célja, az érintettek jogának védelme, beleértve különösen a személyes adatokhoz való hozzáférést, valamint azok helyesbítésének, törlésének és az adatkezelés korlátozásának térítésmentes kérelmezésére és adott esetben megszerzésére szolgáló lehetőségeket. A harmadik pillér az európai adatvédelmi reformban az e-privacy rendelet, amelynek célja a telekommunikációs adatkezelésre vonatkozó szabályok EU rendelet szintű rögzítése. Az egységes jogalkalmazást és a rendeletből fakadó feladatokat – amelyek a nemzetei felügyelő hatósághoz kerülnek – erősíti, ha a 2009/136/EK (2002/22/EK) irányelv[102] helyett ez a terület is rendeleti formában kap új szabályozást. Az irányelv szerint alapvető követelmény, hogy a felhasználóknak kérelmükre megfizethető áron csatlakozást kell biztosítani a helyhez kötött nyilvános hírközlési hálózathoz. A követelmény vonatkozik különösen a helyi, a belföldi és a nemzetközi hívások, az adatszolgáltatások biztosítására. További követelmény a helyhez kötött, nyilvános információs hálózathoz történő csatlakozásnak képesnek kell lennie az online szolgáltatásokra, különösen a nyilvános internet útján nyújtott online szolgáltatásokhoz való hozzáféréshez megfelelő sebességű adatátvitelre. A fogalommeghatározásokat modernizálni kell, hogy azok megfeleljenek a technológiasemlegesség elvének, és lépést tartsanak a technológiai fejlődéssel. A hálózatok integritásának és biztonságának megőrzésével a végfelhasználónak lehetőséget kell adni annak eldöntésére, hogy milyen tartalmat kíván küldeni és fogadni, valamint hogy mely szolgáltatásokat, alkalmazásokat, hardvert és szoftvert kíván használni. A fogyasztókat tájékoztatni kell személyes adataiknak előfizetői névjegyzékben történő felhasználásához kapcsolódó jogaikról, a névjegyzékek céljáról és egyben díjmentesen kérhetik, hogy ne kerüljenek bele nyilvános előfizetői névjegyzékbe. Továbbá biztosítani kell, hogy a végfelhasználók az igényeiknek megfelelő minőségű szolgáltatáshoz jussanak és a felhasználónak a segélyhívó szolgáltatásokhoz megszakítás nélkül hozzá lehessen férni. Az IP-

[101] EURÓPAI TANÁCS 2008/977/IB KERETHATÁROZATA (2008. november 27.) a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről

[102] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2009/136/EK IRÁNYELVE (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról

címek felhasználásában bekövetkező változásokat szigorúan figyelemmel kell kísérni. E tekintetben figyelembe kell venni a vonatkozó irányelv (95/46/EK 29. cikke alapján létrehozott, az egyéneknek a személyes adatok feldolgozása tekintetében való védelmével foglalkozó munkacsoport) következtetéseit és javaslatait (a későbbiekben a GDPR rendelet szabályait). A technológiai fejlődés adatgyűjtő és azonosító eszközökön alapuló alkalmazások fejlesztését teszi lehetővé, amelyek lehetnek rádiófrekvenciákat használó, vezeték nélküli eszközök is. A technológiák alkalmazása során biztosítani kell az egyének alapvető jogainak védelmét, különösen a magánélet és az adatvédelem tiszteletben tartásához való jogot. A szolgáltatást nyújtónak megfelelő műszaki és szervezeti intézkedéseket kell tennie szolgáltatásai biztonságának garantálása érdekében. A nemzeti hatóságoknak támogatniuk kell a polgárok érdekeit, különösen a személyes adatok és a magánélet magas szintű védelmének biztosítását. A nemzeti hatóságoknak ellenőrizniük kell a meghozott intézkedéseket. A személyes adatok kezelése tekintetében az adatkezelők kötelezettsége a megfelelő műszaki és szervezési védelmi intézkedések gyakorlati megvalósítása pl. az adatveszteség elkerülése érdekében. A személyes adatok megsértése (adatsérülés, adatszivárgás, adatokkal való visszaélés és egyéb incidens) jelentős gazdasági veszteséget és társadalmi kárt okozhat az érintett előfizető vagy személy számára. A magánélet védelme, valamint az elektronikus hálózatokon továbbított vagy feldolgozott személyes adatok megfelelő szintű biztonságának megvalósítása érdekében rendelkezni kell a szükséges és elfogadott végrehajtási intézkedésekről (tájékoztatási, értesítési és technikai követelmények). Továbbá megfelelő figyelmet kell fordítani a személyes adatok jogsértésének körülményeire (például a hatékony és részletes kivizsgálás során). Biztosítani kell minden felhasználó magánszférájának magas szintű védelmét. Az úgynevezett kémszoftverek titokban rögzítik a felhasználói tevékenységet, továbbítják harmadik félnek, és súlyos fenyegetést jelentenek a felhasználók magánéletére nézve. A felhasználók világos és átfogó információkkal (például sütik kezelése) kell, hogy rendelkezzenek, mielőtt olyan tevékenységekbe kezdenek, amely egy nem kívánatos hozzáférést és incidenst eredményez. Az előfizetők magánélethez való joga kiterjed a telekommunikációs SMS, MMS vagy egyéb üzenetküldésre szolgáló alkalmazásra is. Az elektronikus rendszerek elterjedésével egyre inkább megnőtt az elektronikus adatok tárolásának, feldolgozásának, kezelésének és továbbításának jelentősége, ami érintette a hivatali, ipari és vállalati, valamint a személyes adatokat is. A személyes adatokra, illetve azok tárolására és kezelésére, immár nemcsak az adóhivatal, a bank, a nyugdíjpénztárak, a helyi és állami hivatalok, de a kereskedelem, a turizmus, úgymint a szálláshelyek és utazási irodák, valamint a helyi cipőbolt tulajdonos is

igényt tart hivatali ügyek intézése és értékesítés, valamint kedvezményérvényesítés célzattal. Sok esetben önként adjuk meg adatainkat a közösségi oldalakon. Az információs rendszerek napi szintű használata indokolttá tette az adatvédelmi alapelvek törvénybe iktatását, az alapelvekre épített szabályozási rendszer kialakítását mind törvényi mind informatikai technológiai szintű megvalósítását. Az alapelvek megvalósítás nélkül csak elmélet maradna, hiszen az adatvédelmi és az információbiztonsági törvényi szabályozási és a fejlett, szabályozott informatikai technológiai rendszer mellé becsatlakozó felhasználói biztonságtudatos viselkedés hármas tényezője, egymást erősítve, hatékony és eredményes együttműködéshez vezethet.

2.4. AZ INFORMÁCIÓBIZTONSÁG JELENTŐSÉGE, JOGTÖRTÉNETE ÉS HAZAI SZABÁLYOZÁSA

2.4.1. AZ INFORMÁCIÓBIZTONSÁG JELENTŐSÉGE

Az információvédelem és az információbiztonság szabályozásának kialakulása, fontossága elsősorban a katonai rendszereknél jelentkezett és alkalmazás szempontjából a II. Világháborúban komoly áttörést jelentett egy-egy katonai művelet esetében. Tekintettel arra, hogy az információ – tudás – hatalom hármas lényegi összefüggéseket tartalmaz, a fontos vagy titkos információt – bár ilyen módon az ókorban még nem azonosították – megfelelő biztonsággal kellett kezelni, tehát védelem alá kellett helyezni. Már az ókorban is fontos szerepet játszott az információk megszerzésére vagy annak megakadályozására irányuló tevékenység, a mai szóhasználattal élve az információvédelem. Az információ védelmére irányuló törekvések már a beszéd megjelenésével egy időben, az emberi társadalmak kialakulásával egyidős tevékenység, hiszen már akkor népszerű tevékenységnek számított az információ „eltulajdonítása”, mivel így próbálták meg ellesni a vadászati szokásokat, a túlélési lehetőségeket vagy az ehető növények termesztésére vonatkozó praktikákat.[103] Az információbiztonság története tehát az ősidőkig visszavezethető. Bár a társadalmi és kulturális fejlődéssel a rendelkezésre álló és megszerezhető információk köre, a jelkészletek megjelenésével és az írás elterjedésével megjelenési formája folyton változott, és ennek megfelelően a vonatkozó információmegszerzéshez és annak megakadályozásához tartozó módszerek is állandóan változtak[104], de a lényegét tekintve, miszerint a védelem és a biztonság

[103] Muha Lajos (szerk.), Az informatikai biztonság kézikönyve, Budapest, Verlag Dashöfer, 2000-2005.
[104] Gémes Csaba, Az információbiztonság alapkérdései, Hadmérnök (XII) IV, Budapest, 2017

a birtokosa számára fontos, változatlan maradt. Az ókori társadalmak fejlődése során a különböző jelekből, strukturált közlési mód, az írás megjelenésével már rögzített formában is rendelkezésre állt az információ, ezáltal könnyebben tárolhatóvá, másolhatóvá vált, átlépve az addigi szavak és emlékezőképesség megőrzésének korlátait. Mai napig rendelkezünk ókori írásos emlékekkel, amelyek segítenek megfejteni az akkori társadalmi és mindennapi élet sajátosságait, örökíthetik a hagyományokat és a tudományos, filozófiai és jogi álláspontokat, kutatási eredményeket. Az írás megjelenése elősegítette az ókori társadalmak fejlődését, az irányításban és a működésben meghatározó szerepet töltött be. Az írástudó emberek kiemelkedő rangot kaptak. Az írástudók alacsony száma egyfajta védettséget jelentett, mivel csak kevesen voltak képesek elolvasni és megfelelően értelmezni a küldemények információtartalmát. Az írás megőrzése elősegítette az információ pontos, eredeti tartamlának tárolását és továbbítását az illetékes személy részére. Az információ ilyen fajta tárolásával és továbbításával már jelentéktelenné vált a személyes jelenlét, mivel a hírnökök és a futárok, később a posta és az elektronikus hálózat betöltötte ennek funkcióját. A szóbeli közleményeket az írásos forma váltotta fel. Ez természetesen nem azt jelentette, hogy a szóbeliség jelentéktelen, és teljes mértékben elvetendő. Ma is vannak jelentős szónoklatok, beszámolók, tudományos értekezések, amelyek hozzájárulnak az innovációhoz, de az írásos dokumentálás is létfontosságú megnyilvánulási forma. Az írás megjelenése, csakúgy, mint az elmúlt évtizedekben az elektronikus hálózat és annak eszközeinek megjelenése és napi szintű alkalmazása forradalmasította az információ kezelését, tárolási lehetőségét és továbbítását. Napjaink információs technológiája alkalmas arra, hogy nagy mennyiségű, írott információ sértetlenül célba érkezzen, és a megérkezés és olvasás tényét nyugtázza a küldő részére. Már az ókori államokban megjelentek a kémkedési és ezzel szemben az elhárítási módszerek is. Különböző algoritmusú titkosírások, jelszavas és rejtjelezési megoldások jelentek meg, amely vonzotta a kódmegfejtési és kódfeltörési tevékenységeket is. Az írásos információ megjelenésével és a közlemény továbbításával újfajta kockázat jelent meg, a hírvivő vagy a közlemény elfogása és jogtalan felhasználása, üzenet kicserélése félrevezetés céljából, a címzett és a feladó megtévesztése és az információ hitelességének kétségbe vonása. Az információ nagy mennyiségű rögzítését elősegítette a középkorban feltalált könyvnyomtatási módszer. Az újfajta információkezelési lehetőségek új biztonsági és védelmi technológiák kialakítását, használatát, valamint intézkedéseket vontak maguk után. Védelmét tekintve a füstjelektől, az uralkodói pecséten, a megbízható futáron keresztül, a különféle kódolási típusokon át, a kriptográfia számtalan fajtájával találkozhatunk a történelem különböző

szakaszaiban. Az írást csak az tudta elolvasni, aki ismerte, ők voltak a kiváltságosok. Később a kriptográfia megjelenése hasonló célokat szolgált, mégpedig, hogy egymástól távol lévő emberek biztonságos módon tudjanak üzenetet váltani. Az ókori megfelelője a szteganográfia (ún. rejtett írás). Hérodotosz számol be arról, hogy a perzsa király ellen szövetkezni akaró Hisztaiaeusz leborotváltatta a küldöncének haját, ráírta az üzenetet, majd megvárta, amíg a küldöncének haja újból kinő, így kelhet át a határon. Bár ez abban az időben nagyon ráérő módszer volt, de akkor még volt erre elég idő. A küldönc célba ért, leborotváltatta fejét és megmutatta az üzenetet a címzett Arisztagorasznak.[105] A fenti megoldásokon kívül ismert még a Polübiosz-négyzet, a Caesar-rejtjel, a bibliai kódok, a grand chiffre kódja (a Napkirály, XIV. Lajos legtitkosabb üzeneteinek kódolása), Pázmány Péter és I. Rákóczi György titkosírása, a morzejelek, Vigenère-kód (1918), navahó nyelv használata (navahó indiánok nyelvével való kommunikálás a II. Világháborúban). Történelmünk során tehát tapasztaltuk, hogy az információt védeni kell, védelmére intézkedéseket kell megfogalmazni, és ezeket az intézkedéseket megfelelő iránymutatások mentén kell kialakítani, tehát az információkhoz illetéktelen hozzáférést meggátló szabályozásokat, folyamatokat és megoldásokat kell kialakítani. A megoldások teljesítését és hatékonyságát előre definiált módszer és folyamatleírás mentén ellenőrizni kell. Az eredményekre intézkedést kell készíteni, amelyet hatékonyan vissza kell forgatni a rendszerbe. A védelmi módszereket fejlesztenek ki minden olyan rendszerre, amely információt tartalmaz, ezáltal tudjuk fenntartani, vagy tovább fejleszteni. A fejlesztés egy adott körfolyamat mentén hajtható vége, amelyet az információbiztonsági szabványok is megfelelően tükröznek. Az informatika fejlődésével együtt alakult ki annak védelmi igénye is, amelyet megpróbáltak később szabályozási keretek közé illeszteni. A szabályozási törekvések immár túlmutattak a haditechnika, a hírszerzés és a védelmi intézkedések határain túl, hiszen ma már behálózza az egész országot, földrészt, illetve a fejlett társadalmak infrastruktúráját, irányítását és működését is. A kommunikáció szabályozása és gyakorlati megvalósítása vonatkozik a közszolgálati és a vállalati információs rendszerekre egyaránt. Az alkalmazott megoldás az ITIL (Information Technology Infrastructure Library), ami lényegében egy szabályozás, illetve az informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan és ajánlás megnevezése. Az ITIL eredetileg BS[106] 15000 jelöléssel brit szabvány és kormányzati ajánlás volt, és a közigazgatási területen meg is követelték ennek alkalmazását. Az ITIL időközben nemzetközi szabvánnyá vált,

[105] Herodotus, „The Histories", London, England: J.M. Dent & Sons, Ltd, 1992.
[106] British Standard

világszerte felhasználói szervezeti támogatást meghatározó módszertanná fejlődött az informatikai infrastruktúra és informatikai szolgáltatás és annak irányítása területén. A szabványt számos nemzetközi informatikai cég is elfogadta és alkalmazta (mint például a HP – Hewlett Packard, Microsoft, vagy az IBM). Az ITIL Biztonságirányítás (Security Management) kiadása a BS7799 brit szabványt használta utalásként, az ITIL folyamatok biztonsági irányítás kiegészítéseként.[107] Az információbiztonság szabályozására vonatkozó jelentősebb ajánlások mai változata a Nemzetközi Szabványügyi Szervezet[108] és a Nemzetközi Elektrotechnikai Bizottság által jóváhagyott és kiadott ISO/IEC 27002: 2013 szabvány, amelynek alapját képező BS7799 eredetileg a Brit Szabványügyi Hivatal[109] által kiadott brit szabvány. Ennek előzményei az 1987. májusában alapított brit DTI/CCSC[110] tevékenységéhez nyúlnak vissza, amelynek feladata volt a nemzetközi szinten is elfogadható informatikai biztonság értékelési és tanúsítási kritériumok és mechanizmus kidolgozása. A DTI/CCSC másik feladatában a brit számítógép felhasználók támogatását tűzte ki célul, amely 1989-ben *A Users Code of Practice* címen került kiadásra, mint az informatikai biztonság megteremtésére és fenntartására vonatkozó legjobb gyakorlatot leíró dokumentum. A brit Nemzeti Számítóközpont az ipari terület felhasználóiból szervezett konzorcium bevonásával ezt továbbfejlesztette. Az eredmény a PD 0003 jelű BSI ajánlás tervezet lett *A Code of Practice for Information Security Management, Az információbiztonság menedzsmentjének gyakorlati kódexe* címmel, a dokumentum IT szakemberek és felhasználók közös munkájával tovább fejlesztésre került, és végül a BSI 1995-ben BS7799 szabványként adta ki. Később a szabvány az informatikai biztonság menedzsment résszel bővítették. A BS7799 második része *Az információbiztonság menedzsment rendszerének specifikációja* (Specification for Information Security Management Systems) címmel került kiadásra 1998-ban, az első rész kiegészítéseként. A BS 7799 szabvány első felülvizsgálata 1999-ben történt meg, és az első részét nemzetközi szabványként (ISO) történő elfogadásra javasolta BSI. A Nemzetközi Szabványügyi Szervezet 2000. év augusztusában a BS 7799 1. részét változatlan szerkezetben, és gyakorlatilag változatlan tartalommal nemzetközi szabványnak fogadta el ISO/IEC 17799 néven. 2000-ben jelent meg az információbiztonság témakör első igazi nemzetközi szabványa az ISO/IEC 17799. 2005-ben egy nagy szabványszám- és jelzet váltás következményeképpen létrejött a ma ismert ISO/IEC 27000 szabványcsalád, ami a nemzetközi szabványosítás területén egy kiemelt, speciális

[107] Muha Lajos, Informatikai biztonsági szabványok és irányelvek, GDF, Budapest, 2006.
[108] International Standard Organization, ISO
[109] British Standard Institute, BSI
[110] DTI/CCSC, Department of Trade and Industry's, Commercial Computer Security Centre (Kereskedelmi és Ipari Minisztérium, Kerekedelmi Számítógép Biztonsági Központ)

témakörnek van fenntartva, az információbiztonság és annak menedzselése, amely tartalmazza a tervezésre, a kiépítésre, a fejlesztésre és fenntartásra valamint az ellenőrzésre vonatkozó nemzetközi ajánlásokat. Az ajánlásokból származtathatók a hazai és az Európai ajánlások, irányelvek, utasítások, előírások és törvények.[111] Mindezen szabályozási törekvéseket az elmúlt években komolyabb európai, illetve ma már elmondható, hogy világszintű szabályozási rendszer követett, ami érinti elsősorban a közszolgálati információs rendszereket állami, valamint a gazdasági rendszereket nagyvállalati szférában. Az intézményeknek és szervezeteknek adaptálnia kell az elektronikus információkezeléssel összefüggő szabályozási rendszert a szervezet által megalkotott előírásokban és a gyakorlati alkalmazásokban egyaránt (elektronikus információ áramlása[112] és védelme[113], GDPR). Az információbiztonsági szabványi (ISO/IEC 27001) ajánlás lényegében egy követelményrendszer az információbiztonsági irányítási rendszer kialakítására, bevezetésére, fenntartására illetve információbiztonsági tevékenység fejlesztésére. Az ajánlás nemcsak azoknak szól, akik egy információbiztonsági irányítási rendszert szeretnének bevezetni, kialakítani, hanem útmutatóul szolgál az Európai Uniós (EU) és a magyar jogszabályok kialakításához is. A szabványi szakkifejezéseket átültették az EU-s irányelvekbe és a magyar jogforrásokba is.

2.4.2. AZ INFORMÁCIÓS TECHNOLÓGIAI PARADIGMA

Az információ elméletben és gyakorlatban is napjaink szerves része, a kapcsolódó kutatások több szinten, így a filozófiai vagy a műszaki szintéren is megtalálhatóak. Kétségtelen, hogy a vonatkozó tudomány sok embert vonz. Azonban nem valószínű, hogy a legtöbb ember világosan meg tudja fogalmazni, milyen az információs világhoz tartozó tudomány. Vannak, akik azt gondolhatják, hogy az elektronikus információelmélet vagy a műszaki tudományok, míg mások azt mondják, hogy egy átfogó, bonyolult értelmezés, amely foglalkoztatja az informatika, a távközlés, az elektronikus eszközök és technológiák tudomány területeinek kutatóit, valamint a genetikai vagy a mérnöki szakembereket is. Mivel a vélemények ettől a ponttól eltérnek, jelenleg nem lehet egyértelmű következtetést levonni, mi az az információ és lényegében mely tudományághoz tartozik.[114] Napjaink társadalomkutatóinak álláspontja szerint az ipari társadalomból az információs társadalomra való áttérés már az 1970-es években

[111] Muha Lajos, Szádeczky Tamás, Irányítási rendszerek, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 2014
[112] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
[113] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
[114] Xue-Shan Yan, Information Science: Its Past, Present and Future, Department of Information Management, Peking University, Beijing 100871, China, 2011.

elkezdődött[115], ahol a hálózati társadalom a hálózat köré épül, a folyamatos információáramlást a hálózati technológiával biztosítják. Az új technológia befolyásolja a társadalom társadalmi, gazdasági és politikai szereplőinek egymáshoz való viszonyát, ezért hatást gyakorol a szereplők tevékenységeire, ezáltal egészen újfajta gazdaság, egyedi fejlődési mód jelenik meg. A gyors tájékoztatás és az információ jelentősége megnőtt, amely egyben a hálózatépítés kritikus jelzőjévé vált. Az információs társadalom egy olyan új, speciális megnyilvánulási forma, amelyben az információ előállítása, feldolgozása, továbbítása alapvető jelentőséggel bír korunk gazdasági és társadalmi rendszereiben. A fizikai és a szellemi munkaerő aránya, úgymond a szellemi vagy más néven a „*tudásmunkás*" nagyobb mértékű megjelenésével jelentősen megváltozott. A szellemi tevékenységek, így a kutatási tevékenységek értékelése is megnőtt a termelési tevékenységben az előállított termék értékének nagy részét immár a befektetett szellemi tőke teszi ki és csak kis hányada az alapanyag. A hálózati paradigma is egészen újszerű formában mutatkozik meg, mivel a korszerű, elektronikus és interaktív kommunikációs eszközök megjelenésével és széles körű elterjedésével új megvilágításba került. A gépek és az elektronikus világ forradalmasítása nemcsak a termelési folyamatokat rövidítette le, de az innovációs lánc idejét is. Az elektronikus hálózat a technika modernizálódásának köszönhetően behatolt és széleskörűen, valamint exponenciális gyorsasággal szétterjedt a társadalom különböző rétegeiben, így a gazdaságban, a kultúrában, a politikában, az élet valamennyi részébe, megalkotva ezáltal a hálózat egy egészen új megjelenési formáját.[116] Az innovációs láncolat időtartamának csökkenése az infokommunikációs technológiát is érinti. A posztindusztriális társadalomban három dimenziónak van jelentősége[117] és ezek közül is az árutermelőről a szolgáltató társadalomra váltás, valamint az elméleti tudás rendszerezésének központi szerepe a műszaki újításokban igazolja az információs technológiai paradigma elméleteket. Az új, intellektuális technológia a rendszerelemzés és a döntéselmélet alapvető eszköze. A szolgáltatói társadalom megvalósulása számszerű adatokkal is alátámasztható, hiszen például az Egyesült Államok 1970-es adata szerint már akkor a munkavállalók 65 százaléka a szolgáltatóiparban dolgozott, míg az árutermelésben vagy az építőiparban 30 százalék és a mezőgazdaságban csupán 5 százalék. Ezzel szemben az ipari társadalmak a szolgáltatások nagy részét az árutermelést kiszolgáló ágazatok, így szállítási, közmű és

[115] Manuel Castells, Az információ kora. Gazdaság, társadalom és kultúra, trilógia, A hálózati társadalom kialakulása, 1996., Az identitás hatalma, 1997., Az évezred vége, 1998.
[116] Hendlein Teréz, Prazsák Gergő, A hálózati társadalom receptje, Gondolatok Manuel Castells „A hálózati társadalom kialakulása" című könyvéről, 2005.
[117] Daniel Bell, Az információs társadalom társas keretrendszere, Információ és távközlés a posztindusztriális társadalomban, Információs Társadalom, I. 3-33., Budapest, 2001. (fordította: Rédey Szilvia, Földvári Balázs)

pénzügyi tevékenységek tették ki. (négy fő szektor foglalkoztatottsági aránya az USA-ban) A mai, posztindusztriális szolgáltatások már más jellegűek, jobban koncentrálódnak a humán jellegű, így az egészségügyi, szociális, oktatói, valamint a professzionális, mint például a rendszerszervezői, informatikai, közigazgatási szolgáltatásokra. Minden ágazat jelentős mértékben támaszkodik az információs, hálózati technológiára és rendszerszervezésre, -támogatásra. A hálózati rendszerek támogatásával az elméleti tudás kodifikációja új társadalmi változást hozott, és a társadalmi változások új, szellemi irányítójává vált. A tudomány, a mérnöki tevékenység határa elmosódik, ahol a tudomány fejlődése segíti az ipart és a mérnöki eredmények további kutatásokat generálnak mind elméleti, mind gyakorlati szinten. Az elméletek összekapcsolódása és alkalmazhatósága megnőtt, új lehetőségek, új termékek és újabb felfedezéseket, kutatásokat, szakosodást hozott. A huszadik század második felében a megjelentek, elterjedtek és megnövekedtek a rendszerezett komplexitás elméletével foglalkozó tudományágak és módszertanok, így például az információelmélet, a kibernetika, a döntéselmélet, a haszonelmélet, a sztochasztikus folyamatok. Ezek szakterületei és tudományos kutatási olyan jelentős módszereket dolgozott ki, mint a Markov-lánc, a lineáris programozás vagy a statisztikai döntéselmélet. A tizenkilencedik század egyik meghatározó tényezője az elektromosság, a huszadik századot pedig a számítástechnika, azaz „analitikus motor", ami befolyásolta. A hálózatban kötött számítástechnikai eszközök ma már minden fejlett országban elérhetőek. A számítógép lett a napjaink társadalmainak igazgatási eszköze is, amely rendszerezi és feldolgozza a sokasodó tranzakciót, adatot és egyéb információt, amely például a közigazgatási irányításhoz, államigazgatáshoz is elengedhetetlen. A társadalmi kapcsolatok, tranzakciók és egyéb információk száma az elektronikus rendszerekben évről évre exponenciálisan nő, optimális kezelhetősége viszont már a jövő generáció problémája. Manapság egy üzleti vagy egy közigazgatási szervezet életében egyre inkább domináns helyet foglal el az intellektuális technológia és az posztindusztriális társadalom központi tényezője az intellektuális technológia. (2. táblázat) Az információs technológiai paradigma elmélete szerint az alapanyag maga az információ, további jellemzője az áthatóság, újabb és újabb egymásra épülő hálózati logika - ebből eredően nagyfokú rugalmassággal bír -, valamint a speciális technológiák növekvő konvergenciája állapítható meg, amelyek erősen integrált rendszerhez vezethetnek.

	Preindusztriális	Indusztriális	Posztindusztriális
Termelési mód	Kitermelő	Termelő	Feldolgozó; újrahasznosító
Gazdasági szektor	**Elsődleges** Mezőgazdaság Bányászat Halászat Favágás Olaj és gáz	**Másodlagos** Árutermelés Gyártás Tartós iparcikkek Nem tartós iparcikkek Építőipar	*Szolgáltatások:* **Harmadlagos:** Közlekedés, Közüzemek **Negyedleges:** Kereskedelem, Pénzügy, Biztosítás, Ingatlan **Ötödleges:** Egészségügy, oktatás, kutatás, kormányzat, kikapcsolódás
Átalakulást hozó erőforrás	**Természetes energia** Szél, víz, igásállatok, emberi izomerő	**Gyártott energia** Áram, olaj, gáz, szén, atomenergia	**Információ** Számítógépek, adatátviteli berendezések
Stratégiai erőforrás	Nyersanyagok	Finánctőke	Tudás
Technológia	Kézműipar	Gépi technológia	Intellektuális technológia
Tudásbázis	Kézműves, fizikai munkás, gazda	Mérnök, betanított munkás	Tudós, műszaki és professzionális foglalkozások
Módszertan	Józan ész, próba-szerencse; gyakorlat	Empiricizmus, kísérletezés	Absztrakt elméletek, modellek, szimulációk, döntéselmélet, rendszerelemzés
Időperspektíva	Múltorientált	Ad hoc alkalmazkodó képesség, kísérletezés	Jövőorientált: előrejelzés és tervezés
Tervezés	Játék a természet ellen	Játék a mesterséges jövő ellen	Személyek közötti játék
Vezérelv	Hagyományközpontúság	Gazdasági növekedés	Elméleti ismeretek kodifikációja

2. táblázat, Posztindusztriális társadalom összehasonlító táblázata, Az információs társadalom társas keretrendszere, Daniel Bell (Információs Társadalom, I. 16., Budapest, 2001.)[118] alapján saját szerkesztés

Összességében megfogalmazható, hogy a „*többszörösen rétegződött hálózatként a nyitottság felé tart*”.[119] Az információs technológiai paradigma legfontosabb jellemzői a tudásalapúság, a horizontalitás, a hálózatiság, az adaptivitás, a tanulékonyság, az időtlenség, továbbá a kölcsönös függőség. Az elektronikus hálózat felgyorsult kommunikációt, térbeli távolságok összeszűkülését, a cselekvési idő lerövidülését, a határok kitolódását majd eltűnését eredményezi és ezen kívül még számos előnyt és hátrányt, amely visszahat a társadalomra, a gazdaságra és a kultúrára. A modernebb hálózatok új kommunikációs és média technológiára épülnek, ami forradalmasította az eddigi technológiákat és további kulturális változásokat eredményezett. A virtuális környezet megjelenése innovatív hatással bír, már az oktatásban és a tudomány világában is érezteti hatását. A legfiatalabb generáció interaktív táblák segítségével tanulhat és a hálózat segítségével a Föld más pontján élő hasonló korú és érdeklődésű diákokkal tarthat online kapcsolatot. A tudományok területén hatalmas változást hoz az eredmények azonnali publikálhatósága a világhálón, és azok szinte azonnali felhasználhatósága és

[118] Daniel Bell: Az információs társadalom társas keretrendszere, Információ és távközlés a posztindusztriális társadalomban, Információs Társadalom, I. 16., Budapest, 2001. (fordította: Rédey Szilvia, Földvári Balázs)
[119] Manuel Castells: Az információ kora. Gazdaság, társadalom és kultúra, trilógia, A hálózati társadalom kialakulása, 1996., Az identitás hatalma, 1997., Az évezred vége, 1998.

továbbfejlesztése. Vélhetően a tudományágak társadalomban betöltött szerepe tovább fog erősödni. Az elektronikus hálózat és a gyors információáramlás hátránya, hogy néhány fiatal tudományterületen a tíz évnél régebbi publikáció elavultnak tekinthető. A dinamikusan fejlődő technikai, társadalmi és kulturális változás hatására a kutatásra fordítható idő is lerövidül. Az elektronikus hálózat mindennapos használatával mára már megnőtt az igény arra, hogy a földrajzilag távol élő tudósok és kutatócsoportok együtt dolgozhassanak, ezen kívül természetes igénnyé vált az internet, valamint a szükséges elektronikus eszközök megléte és a szükséges megfelelő szintű szolgáltatása. Természetesen a nem lektorált vagy az interneten nagy mennyiségben megtalálható információk között egyre nagyobb mértékben jelennek meg nem ellenőrzött és nem megbízható adatok is, ezért a tudományos ellenőrzésnek vagy önellenőrzésnek tovább kell erősödnie. Az internet logikája a szabadság eszméjén alapul, amely a mondás szerint „azt tehetünk, amit csak akarunk, akkor és úgy, amikor csak akarjuk". A virtuális világban ez is csak egy illúzió, mivel a dezinformációnak ebben a környezetben is vannak következményei, de egészen más jellegű, mint egy „*face-to-face*" kapcsolat esetében. A túlzott szabadság teret enged az anomáliáknak, mivel a virtuális világ bármely típusú avatar-ja felhasználható, így egy közösségi oldalon bármilyen korú, kinézetű személyiség felhasználható. A résztvevők tudatosan alkalmazhatják az eltérő személyiségeket. Ugyanakkor egyes esetben a külső megjelenés lényegtelen, például egy közösségi csoport kialakulásában és összetartó erejében a bizalom, az, ami felértékelődik, és az összetartó erő kulcsfontosságú tényező lehet.

2.4.3. AZ INFORMÁCIÓBIZTONSÁG JOGTÖRTÉNETE

Az információbiztonság napjaink egyik legösszetettebb és legfiatalabb jogintézménye, ókori eszmékkel a háttérben, modern információs technológiai és jogi vonatkozásokkal. Mint fogalom hosszú utat tett meg a mai formájáig és betöltött szerepéig. A jelenlegi előírásokat figyelembe véve az államigazgatási és közigazgatási szervek kötelezettek arra, hogy többek között az elektronikus információbiztonsági Ibtv. [120] és az Infotv. előírásait együttesen alkalmazzák. „*A biztonság nem egy termék, hanem egy folyamat*." Sőt, a biztonság nem technológiai, hanem emberi és vezetési probléma.[121] Az Ibtv. értelmében az elektronikus információs rendszer biztonsága az adott rendszer olyan állapota, amelyben a védelem zárt a rendszerben nyilvántartott és kezelt adatok, valamint a rendszerelemek bizalmasságára,

[120] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
[121] Kevin D. Mitnick, William L. Simon, The art of deception, 2003

sértetlenségére és rendelkezésre állására. A biztonságos rendszer minden elemével és információjával együttvéve a sértetlenség és a rendelkezésre állás szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. A rendszer zárt, amennyiben az elemzés során minden jelentős fenyegetést figyelembe vesz és kezel. Teljes körű, ha a rendszert alkotó összes elemére kiterjed és folyamatos, ha az időben változó körülmények ellenére is megszakítás nélkül működik és kiszolgálja a szükséges folyamatokat, kéréseket. A rendszer kockázatarányos, amennyiben a feltehető kárérték és a kár valószínűségének szorzata nem haladhat meg egy előre megállapított és rögzített küszöbértéket. A küszöbérték minden esetben az üzleti döntés eredménye. A kockázatikezeléssel kapcsolatban nagyon fontos tudatosítani, hogy nincs, és nem is létezik teljes mértékű biztonság, nemcsak az informatikában, de más területen sem, így a gazdaságban vagy az üzleti tevékenységben sem. A megállapított kockázati érték csak konvergál a teljes biztonsághoz, elérni sosem fogja, így a fennmaradó érték a maradványkockázat. A biztonsági szint növelhető a kockázatkezelés során meghozott szükséges intézkedések végrehajtásával. Az elért és az intézkedések végrehajtásával elérhető biztonsági szintet sok tényező befolyásol, de ezek közül is a legkiemelkedőbb az emberi tényező. Mint az élet más területein is általában, itt is a leggyengébb láncszem az ember. Az információ ebben a kontextusban bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy új ismeret. Lényegét tekintve valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti. Ez a fogalommeghatározás pontosítja és közelebb viszi az információs rendszerhez a latin eredetű meghatározást. A rendelkezések szerint az elektronikus információs rendszert ért biztonsági esemény egy előre nem tervezett, nem kívánt olyan egyedi esemény vagy eseménysorozat, amely a rendszerben kedvezőtlen változást, kárt idéz elő, és amelynek hatására a rendszer által hordozott vagy nyilvántartott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása illetve rendelkezésre állása megsemmisül vagy sérül. A biztonsági eseményt a katasztrófaelhárítási tervnek megfelelően kezelni kell, így szükséges az esemény dokumentálása, a következmények felszámolása, a bekövetkezés okainak és felelőseinek megállapítása és a jövőre vonatkozó hasonló események elkerülésének érdekében az intézkedések megfogalmazása és végrehajtása. További alkalmazandó meghatározások, jogintézmények a kibervédelem és a kiberbiztonság.[122] Az információbiztonsággal kapcsolatos

[122] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.) szerinti fogalom

legfőbb meghatározás a bizalmasság, sértetlenség és a rendelkezésre állás. Az információs világ védelmi szférájához tartozik az információbiztonság is, amely lehet a jelen korunk új „találmánya" vagy akár egy nagyon régi, de pontosan nem meghatározott fogalom divatos köntösben. Ahhoz, hogy megtudjuk a tényleges választ meg kell vizsgálnunk az információbiztonság fogalmát, történelmi vonatkozásait, jelen gyakorlati és jogszabályi helyzetét. Az információbiztonság a jelen kor egyik divatos kifejezése vagy jogintézménye, amelyet szokás összekötni az informatika világával, hiszen az információ az informatika egyik alapfogalma is. Ez a kényelmes megközelítés elfelejtteti velünk azt, hogy nemcsak az informatika szakterületén találkozhatunk információval.[123] Attól függően, hogy milyen modellben, értelmezési szinten, valamint tudományágban használjuk, az információ más-más jelentéstartalommal bír, más-más aspektusa lehet releváns az adott kontextusban. Az információhoz társuló biztonság a dolgok olyan rendje, állapota, amelyben kellemetlen vagy negatív kimenetelű meglepetés szerű eseménynek, zavarnak, behatásnak, veszélynek nincs, vagy alig van bekövetkezési valószínűsége, lehetősége. A jelen álláspontok értelmében az információ és a biztonság együttesen, az információbiztonság a szóban, rajzban, írásban, a kommunikációs, informatikai vagy más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Egy elektronikus információs rendszer biztonságán, például olyan állapotot értünk, amelyben annak védelme a rendszerben kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[124] Érdemes itt megjegyezni, hogy egy rendszer fogalmán szintén sokféle jelentést érthetünk, így lehet könyvek katalogizálása és elhelyezése a polcon, vagy tűzvédelmi rendszer, és nem minden esetben egy elektronikus információs rendszer. A huszadik század második feléig az elektronikus rendszer fogalmának napi szintű használata nem létezett, de az információkutatás vagy információvédelem, különösen a katonai védelem területén, igen.

2.4.4. AZ INFORMÁCIÓBIZTONSÁG ÉS AZ INFORMÁCIÓVÉDELEM

Az információbiztonság az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság, szintén ebbe a témakörbe tartozhatnak.[125] Egy

[123] Muha Lajos (szerk.), Az informatikai biztonság kézikönyve, Budapest: Verlag Dashöfer, 2000-2005
[124] Muha Lajos, Az informatikai biztonság egy lehetséges rendszertana, 2008, Bolyai Szemle, XVII. évf. 4. szám, p. 137-156., Budapest: ZMNE BJKMK, ISSN: 1416-1443
[125] MSZ ISO/IEC 27000:2014 szabványcsalád

információbiztonsági rendszer kiépítése során ezen fogalmakra irányuló alapelvek teljesítése kötelező. A bizalmasság alapelve, amely annak biztosítása, hogy az információ csak az arra felhatalmazottak számára legyen elérhető. Ha megfigyelünk némely katonai stratégiai, történelmi eseményt, megállapítható, hogy fontos szerepet játszott a titkos információ továbbításának irányítása és pontos végrehajtása, hiszen akár egy uralkodó státusza, vagy egy ország sorsa múlhatott ezen. A sértetlenség (integritás) alapelve, az információk és a feldolgozási módszerek teljességének és pontosságának megőrzése. A téves vagy félinformációk, téves döntéshez vezetnek, így a megoldások, a variációk halmaza is bővebb, ami zavart kelthet akármelyik rendszerben, legyen az stratégiai, gazdasági vagy katonai. A rendelkezésre állás alapelve alapján biztosítani kell, hogy az érintett felek mindig hozzáférjenek a megfelelő információkhoz, és akkor, és amikor az szükséges. Mindhárom alapelv elengedhetetlen, akár napjaink információbiztonsági irányítási rendszerének kiépítését, akár bármely történelmi kor közigazgatását, katonai stratégiáját vagy kormányzati irányítását tekintjük. Ugyanakkor az alapelvek meghatározása kellőképpen modern, mégis rendkívül fontosak voltak akár régen, úgy ma is.[126] Az információbiztonsági intézkedések alatt általában az információs rendszerekben tárolt adatok sérülése, megsemmisülése, jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttesét értjük. A bevezetett intézkedéseket két nagy területre lehet bontani adatvédelemre[127] és adatbiztonságra[128]. Információbiztonságot a gyakorlatban például a kontroll módszert alkalmazva, egyes jelentős kérdések megválaszolásával lehet megvalósítani:

- Mit kell megvédeni?
- Mitől kell megvédeni?
- Hogyan kell megvédeni?

Amennyiben a fenti kérdésekre adott válasz ismert, a terület szabályozás alá vonható.

2.4.5. AZ EURÓPAI UNIÓ ÉS HAZAI INFORMÁCIÓBIZTONSÁGI IRÁNYELVEK

Magyarország Kormánya a Nemzeti Infokommunikációs Stratégiájában (a továbbiakban NIS), követve az Európai Unió által előírt követelményeket és irányelveket meghatározta a vonatkozó

[126] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
[127] informatikai vonatkozásban: az informatikai, illetve az információs rendszerek adatvesztés elleni védelmét, az adatok folyamatos rendelkezésre állását biztosító szabályozás, folyamatok és megoldások
[128] : az informatikai, illetve információs rendszerek adataihoz való illetéktelen hozzáférést meggátló szabályozás, folyamatok és megoldások

hazai informatikai és távközlési területeket, azok fejlesztésének lényeges elemeit és a 1069/2014. (II.19.) Korm. határozattal rögzítette a NIS elfogadását. A digitális ökoszisztéma, így a szupergyors internet, a digitális közösség és gazdaság, az elektronikus közszolgáltatások és a digitális készségek fejlesztésének célkitűzéseivel előirányozta a Digitális Magyarország céljainak meghatározását és kivitelezésének súlypontjait. Napjaink hazai digitális fejlesztése komplex feladat, hiszen túlmutat a kapcsolódó szektorok és intézmények elektronikus fejlesztésén, egészen a felsőfokú tudatosításig, valamint a háztartások informatikai képességéig, a szolgáltatások megvalósításáig, a helyi szintű infrastrukturális hálózati adottságokig és a kivitelezhetőség feltételrendszeréig terjed, beleértve minden szükséges tudást és eszközképességét is. A közszolgálati rendszerfejlesztések tekintetében az egyik jelentős cél, egy olyan mértékű feltételrendszer kialakítása, amely megvalósítja különösen a különböző közszolgáltatási szintek kiegyenlített, hatékony együttműködését és az információk közös értelmezésen alapuló, az együttműködési képességet megvalósító információs rendszerek létrehozását és működtetését. A Digitális Magyarország 2014-2020 időtávlatra vonatkozó infokommunikációs területi fejlesztési irányokat, közpolitikai, szabályozási és támogatási teendőket a Nemzeti Fejlesztési Minisztérium által 2014. decemberében kiadott, *Zöld könyv az infokommunikációs szektor 2014-2020 közötti fejlesztési irányairól*[129] című kiadvány tartalmazza. A programok kidolgozásához, megvalósításához és megfelelő eredmények felmutatásához elengedhetetlenül fontos a háttérben kiszolgáló tevékenységet ellátó információs rendszerek interoperabilitása, különösen a közszolgálat területén. A meglévő rendszerek összehangolása és együttműködése nagy feladat és kihívás mind a tervezők, mind a megvalósítók számára. Ezen a területen a már meglévő, közel évszázados – illetve az ISO 70 éves – múltra visszatekintő szabvány[130] [131] alapú elektronikus technológia jelentős segítséget nyújt a rendszerek összeköttetését és rendelkezésre állását biztosító információs technika megvalósításában, de a szintaktikai, valamint a szemantikai megfeleltetés és együttműködés alapvető megoldandó feladatokat támaszt a tervezők és a kivitelezők számára. Elektronikus világunkban az ideiglenes vagy tartós együttműködésre kényszerített informatikai rendszerek alapvető nehézségei az együttműködési szituációkban jelentkeznek, amikor az elektronikai

[129] Zöld könyv az infokommunikációs szektor 2014-2020 közötti fejlesztési irányairól, 75, 81, 93, 139, 140, 142, 144, 147, 154, p, Budapest, 2014. http://www.kormany.hu/download/b/f7/30000/Z%C3%B6ldk%C3%B6nyv%20v%C3%A9gleges.pdf, Letöltés: 2018. június 13.

[130] Magyar Szabványügyi Testület, http://www.mszt.hu/web/guest/a-szabvanyositas-tortenete, letöltés: 2021. november 23.

[131] International Organization for Standardization, https://www.iso.org/about-us.html, letöltés:2022. március 6.

információáramlás és a résztvevők közti információcsere, ugyan ember alkotta irányítással, de mégis, közvetlen emberi közreműködés nélkül valósul meg[132]. Az Európai Interoperabilitási Keretrendszer (EIF)[133] határozta meg az interoperabilitási szinteket, amelynek első szintje a technikai kihívások. Ez az a szint, amely az információs és kommunikációs technológiai (IKT) rendszerek összekapcsolásának műszaki előírásaival, kivitelezésével és egyéb kérdéseivel foglalkozik. Feladata, hogy megoldást találjon azon közszolgálati információs rendszerek, szervezetek, alkalmazások által használt különösen az adatformátumok, az adatsémák és a kommunikációs protokollok által, az adott rendszerek együttműködése során felmerülő kérdésekre, és esetleges problémákra.[134] Az EIF európai közszolgáltatások alapelvei közül az 5. alapelv a technológiasemlegesség és az adathordozhatóság. Az alapelv szerint a műszaki kivitelezést úgy kell megvalósítani, hogy a funkcionális követelmények igényein alapuljon. Fontos, hogy a feladatot megvalósító platformfüggetlen technológiai megoldások tervezése és kivitelezése megoldható legyen, egyúttal figyelembe véve a választott, szabvány alapú technológiák együttműködési képességét. Az együttműködésnek lehetővé kell tenni a szükséges adatok szabad áramlását és könnyű hordozhatóságát, figyelembe véve különösen az adatkezelés, illetve az adattovábbítás Infotv. és a bizalmasság, sértetlenség és rendelkezésre állás Ibtv. elveit és szabályait. Az elveket figyelembe véve nyílt forráskódú rendszerek használatának megvan az a veszélye, hogy a kiberbűnözői szféra is ismeri, és ki is használja a rendszer adta gyengeségeket, biztonsági réseket. Az elvárt, és eredményes műszaki kivitelezést nagymértékben elősegíti a szabvány alapú megoldások használata, ami lehetőséget nyújt arra, hogy az előírások szerint kiválasztott technikai megoldások egymással kompatibilisek legyenek. Az ISO/IEC 27000-es szabványcsalád nemcsak az információbiztonsági általános követelményrendszere, hanem például a hálózat- (ISO/IEC 27033) valamint alkalmazásbiztonság (ISO/IEC 27034) szabványait is tartalmazza, amelyek figyelembe vétele már tervezés során hasznos. Nemcsak ajánlás, hanem stratégia terén is megjelentek az információbiztonság szabályozására irányuló igények. Az Európai Bizottság 2010. év májusában mutatta be az *Európai Digitális Menetrend* stratégiáját (2. végleges változat:

[132] Munk Sándor, A Magyar Honvédség informatikai interoperabilitási politikája, 2006. Ludita, a Nemzeti Közszolgálati Egyetem repozitórium-rendszere

[133] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Európai Interoperabilitási Keret – Végrehajtási stratégia, https://ec.europa.eu/transparency/regdoc/rep/1/2017/HU/COM-2017-134-F1-HU-MAIN-PART-1.PDF, Letöltés: 2018. június 13.

[134] Győrffyné Holló Krisztina, Közszolgálati információs rendszerek interoperabilitási nehézségeinek megoldása, DUNAKAVICS 2021. IX. évfolyam II. szám pp. 21-40. , 19 p., 2021.

2010.08.26.)[135]. A stratégia célja, a gazdasági fellendülés felgyorsítása és a fenntartható digitális jövő alapjainak megteremtése volt. Az intézkedési és cselekvési terv hét kiemelt területet határozott meg, amiben kiemelt szerepet kapott az internet iránti bizalom és a biztonság erősítése. A stratégia további célja, az információs rendszerek ellen irányuló incidensek irreálisan magas számának csökkentése. Az intézkedésekben szerepel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló jogszabály-szigorítás, a gyors reakciójú, integrált európai rendszer létrehozása és működtetése, az Európai Hálózat- és Információbiztonsági Ügynökség által koordinált tagállami forróvonalak létrehozása. Az utóbbi a gyerekek és szüleik bejelentésére, a tudatosságnövelésre az iskolákban, a gyermekbántalmazással, a személyazonosság-lopással és számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozására, a magánélethez- és a személyes adatok védelméhez való jog érvényesítésére irányult. A stratégia hatására 2013-ban az Európai Unió intézményei létrehozták a CERT-EU[136] szervezetét, valamint létrejött az Európai Parlament és a Tanács 2013. május 21-i, 526/2013/EU rendelete, és felállításra került a Számítástechnikai Bűnözés Elleni Európai Központ és az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban Ügynökség, ENISA, Kréta, Iráklio székhellyel). Az 526/2013/EU rendelet kiemeli az elektronikus szolgáltatások, valamint a magánélet és a személyes adatok védelmére irányuló fokozottabb fellépési igényeket.[137] [138] Az Európai Bizottság az Európai Parlamentnek címzett

[135] Az európai digitális menetrend, http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=COM:2010:0245:FIN, letöltés: 2021. december 4.

[136] Computer Emergency Response Team (CERT-EU) for the EU institutions, 2012. szeptember 11. után létrejött ügynökségek és szervek, https://cert.europa.eu/cert/plainedition/en/cert_about.html

[137] „*Működési zavaraik jelentős fizikai, társadalmi és gazdasági kárt okozhatnak, ami rámutat azoknak az intézkedéseknek a fontosságára, amelyek a kritikus szolgáltatások folyamatosságának biztosítása érdekében ellenálló képességük növelését célozzák. Az elektronikus hírközlés, az elektronikus infrastruktúra és az elektronikus szolgáltatások – különösen integritásukat, rendelkezésre állásukat és titkosságukat tekintve – egyre nagyobb kihívásokkal néznek szembe, amelyek többek között a hírközlési infrastruktúra egyedi alkotórészeihez, és az alkotórészeket szabályozó szoftver elemeihez, az általános infrastruktúrához és az infrastruktúrán keresztül nyújtott szolgáltatásokhoz kapcsolódnak. Mindez egyre nagyobb aggodalommal tölti el társadalmunkat, nem utolsósorban azért, mert a rendszerek összetettsége, a működési zavarok, a rendszerhibák, a balesetek, az emberi hibák és a támadások olyan problémákat okozhatnak, amelyek az európai polgárok jóléte szempontjából kritikus jelentőségű szolgáltatásokat közvetítő elektronikus és fizikai infrastruktúrára is kihathatnak.*”
„*A magánélet és a személyes adatok magasabb szintű védelme érdekében az Ügynökségnek hozzá kell járulnia a magas szintű hálózat- és információbiztonság megteremtéséhez, illetőleg az Unió polgárai, fogyasztói, vállalkozásai és közszektorbeli szervezetei javára részt kell vennie a hálózat- és információbiztonság kultúrájának kialakításában és előmozdításában, mindezzel pedig elő kell segítenie a belső piac megfelelő működését.*”
Az Európai Parlament és a Tanács 526/2013/EU rendelete, az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről, 2013

[138] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), letöltés: 2019. november. 23.

a 2016.5.30-i COM(2016) 363 final közleménye alapján javasolta[139] [140] a hálózat- és információbiztonság területén illetékes hatóságok létrehozását (NIS), a számítógép-biztonsági eseményekre reagáló csoportok felállítását (CSIRTs), a nemzeti hálózat- és információbiztonsági stratégiák és együttműködési tervek elfogadását (NIS)[141]. A magyarországi törekvések sem maradtak el a nemzetközi szabályozástól, hiszen joggal elmondható, hogy az információbiztonságot érintő hazai törvényi szabályozás, melyet az Európai Unió és tagállamai tekintetében Magyarország elsők között alkotott meg és léptetett hatályba, összhangban van az uniós elvekkel és elvárásokkal.[142] Az Európai Interoperabilitási Keretrendszer (EIF) által meghatározott jogszabályi megfelelőség előírásai jogszabályi úton támogatja a közszolgáltatás információs rendszereinek interoperabilitási elveit, technikai megvalósítását és szabályait. [143] Az információs rendszerek interoperabilitásának kivitelezése során az adatvédelmi és más jogi követelményeket szigorú előírásként kell kezelni, nem a szereplők kényelmét, hanem a törvényi eljárások hatékony végrehajtásához elengedhetetlen információk áramlását kell segíteni. A támogatási megoldások kiterjednek a rendszerekhez kapcsolódó hozzáférési szintek, jogosultságkiosztások hozzáférések engedélyezési eljárására és részletesen naplózott elvi és gyakorlati eljárásaira. A jelen értekezésben hivatkozott jogszabályokon kívül, a közigazgatási adatbázisok összekapcsolásának szükségességét a döntés előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény[144] is szabályozza. A szabályozás tartalmazza az anonim kapcsolati kód kialakítására vonatkozó előírásokat, a kódképzés alapját és az adatbázis felhasználhatóságát. A fentieken kívül, a két legfontosabb adatvédelmi szabályozás, az elektronikus azonosítást[145] és a személyes

[139] 2013/0027/COD, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148, letöltés: 2022. március 6.
[140] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148, letöltés: 2019. június 1.
[141] További javaslat „*A konkrét kritikus ágazatokban működő vállalatoknak és a közigazgatásoknak ezentúl fel kell mérniük az őket fenyegető kockázatokat, majd megfelelő és arányos intézkedéseket kell alkalmazniuk a hálózat- és információbiztonság garantálása érdekében.*"
[142] Közigazgatási Informatikai Bizottság, Magyar Informatikai Biztonsági Keretrendszer (MIBIK - KIB 25. sz. ajánlása 1.), Informatikai Biztonsági Irányítási Rendszer (IBIR - KIB 25. sz. ajánlása 1-1.), az Informatikai Biztonság Irányítási Követelmények (IBIK - KIB 25. sz. ajánlása 1-2.), Informatikai Biztonság Irányításának Vizsgálata (IBIV - KIB 25. sz. ajánlása 1-3.)
[143] Európai Bizottság: Európai interoperabilitási keret – Végrehajtási stratégia (2017), https://ec.europa.eu/transparency/regdoc/rep/1/2017/HU/COM-2017-134-F1-HU-MAIN-PART-1.PDF, letöltés: 2021. december 10.
[144] 2007. évi CI. törvény, a döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról
[145] Az európai parlament és a tanács 910/2014/eu rendelete, http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32014R0910, letöltés: 2021. december 20.

adatok védelmét[146] tekintik elsődlegesnek. Az utóbbi szabályozás Magyarországon 2018. májusában lépett hatályba, amely jelentősen befolyásolja, szigorítja a hazai, az európai és az Európai Unión kívüli elektronikus adatforgalmat, és a szabályok be nem tartása jelentős anyagi következményekkel járhat.

2.4.6. INFORMÁCIÓBIZTONSÁGI SZABÁLYOZÁS AZ EURÓPAI UNIÓBAN

Az információs technológiák mindenütt jelen vannak, és megváltoztatják életünket, valamint munkavégzési szokásunkat. A digitalizálás példátlan új lehetőségeket teremtett, számítunk a mindennapos jelenlétére és elősegíti társadalmunk fejlődését és a demokratizálódást. Az erő, ami az információs technológiákban rejlik sokszor csak egy élménydús, fantasztikus, mindennapi játék, máskor pedig felbecsülhetetlen károkat okozó fenyegetettség, ezért szabályozása elengedhetetlen. Napjainkban immár világszintű törekvés az információ védelme mind szabályozási mind pedig gyakorlati szinten. A világ informatikai szempontból fejlett társadalmai, így az amerikai, európai és a távol keleti országok információs társadalmának biztonsága és megfelelő védelme érdekében egyre több nemzeti, Európai Uniós és nemzetközi egyezményeket, stratégiákat és intézkedéseket fogalmaznak és valósítanak meg. Az intézkedések szükségességének kiindulópontja nemcsak az ipari fejlődés, az ipar 4.0 keretén belül előforduló kutatások vagy fejlett technológia védelme, hanem az információs rendszerek, azok technológiai folyamatai és a bennük tárolt vagy közlekedő információk védelme a fokozódó fenyegetésekkel szemben. Az adatainkat ért támadásokkal immár napi szinten számolni kell a kormányzati, az ipari, az üzleti és a magánszférában egyaránt. Ha a legveszélyesebb fenyegetéseket megvizsgáljuk, előtérbe kerül az egyre fokozódó információs terrorizmus, amely elsősorban a virtuális térben fejti ki hatását. Sokszor olyan technológiákat alkalmaznak, ami által tevékenységük megfoghatatlan, követhetetlen és egyes szervezetek számára felderíthetetlen. Tevékenységük nem ismer határokat, így, ha utat tör, sem ország, sem földrész határ nem létezik számukra. A szervezetek jó része olyan technológiával rendelkezik, amely képtelen az információs csatornán megjelenő illetéktelen azonnali beazonosítására és hatástalanítására. Sokszor egy utólagos analizálás során derül fény a kár mértékére. A kormányzati, ipari és lakossági adatok biztonságának érdekében meghozott nemzeti és nemzetközi információbiztonsági szabályozási rendszer és intézkedések célja a társadalom

[146] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679, letöltés: 2021. december 20.

működésének támogatása létfontosságú információs infrastruktúrával, amelynek működtetése és védelme is elengedhetetlen. Az információs vagyon védelemének érdekében szabványokon alapuló törvényi, jogszabályi és technológiai törekvéseket tapasztalhatunk, és egyre több olyan szervezet jön létre a kormányzati és az ipari szférában egyaránt, amely az információbiztonsági törekvéseket, az informatikai biztonságot hivatott erősíteni, szabványi és jogszabályi előírásokat vegyítve a fejlett informatikai technológia alkalmazásával. A támogatáshoz elengedhetetlen a jogszabályok összhangja, amelyeket az Európai Unió tagállamai és más, fejlett nemzetek igyekeznek biztosítani. Európában a hálózati és információs rendszerek használata széles körben elterjedt, nemcsak a közintézmények, a vállalkozások, hanem a polgárok napi szintű használatává vált. A folyamatosan terjedő szolgáltatások és termékek szervezeti és fogyasztói szintű használatához elengedhetetlen a digitalizálás, és az információs rendszerek összekapcsolása, az internet napi szintű használata. Egyre növekvő számú információs eszköz kapcsolódik az internethez, de sajnos még mindig elmondható, hogy ezen eszközök esetében nincs kellőképpen beépítve a biztonság- és ellenállóképesség, amely nem megfelelő információbiztonsághoz vezet. Az információs rendszerek tanúsításának korlátozott alkalmazása következtében sem a magán, sem pedig az intézményi, vagy az üzleti felhasználók nem rendelkeznek elegendő információval az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok információbiztonsági jellemzőiről. A bizonytalanság vagy információhiány aláássa a digitális megoldásokba vetett bizalmat. Az információs rendszerek képesek életünk minden területét segíteni, akár egyéni, akár szervezet szinten, így összességében megállapítható, hogy képesek a vállalkozások működését élénkíteni, és a gazdaság növekedését ösztönözni. Az IKT által támogatott rendszerek a digitális egységes piac megvalósításának sarokkövét jelentik. [147]
A szabályozási rendszerekre általában elmondható, hogy az információbiztonságot és az adatvédelmet külön kezelik. Igy van ez az Európai Unióban és tagállamaiban, ahol például a GDPR iránymutatást és alapot ad a tagálamok információs önrendelkezési jog szabályozására. Az információbiztonsági szabályozási célkitűzéseknek megfelelően figyelembe kell venni az információbiztonságra vonatkozó jogszabályi előírásokat, amelynek vonatkozó alap– és irányelvei az ISO/IEC 27000-es információbiztonsági szabványcsalád dokumentációjában, követelményrendszerként található meg. A jelenleg érvényben lévő jogszabályok ötvözik az információbiztonsági szabványok ajánlásait, a kiépítésre és működtetésre vonatkozó

[147] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), letöltés: 2019. november 23.

módszertanokat (különösen a COBIT[148], a CRAMM[149]) és szakspecifikumokat, valamint a közigazgatási irányelveket. Az Európai Unió szabványosításról szóló rendeletében elfogadta a nemzetközi szabványok használatát és lehetővé tette az Unió és a nemzetközi szabványügyi testületekkel való együttműködést.[150] [151] A rendelet olyan termékekre és szolgáltatásokra vonatkozó európai szabványokra épülő szabályokat, IKT műszaki előírásokat állapított meg az európai szabványügyi szervezetek, a nemzeti szabványügyi testületek, a tagállamok és az Európai Bizottság közötti együttműködés, az Európai Uniós jogszabályok és politikák végrehajtása érdekében, amelyekre hivatkozni lehet, az IKT terület finanszírozása és a szakmai szervezetek szükséges bevonása tekintetében. Az európai szabványosítás egységesíti az európai IKT eszközök működését, innovációját és azok gyors kommunikációját, interoperabilitási képességüket egy olyan virtuális térben, ahol az országhatárok nem képeznek akadályt, ezáltal elősegíti a vállalkozások versenyképességének növelését is, és megerősíti az európai ipar globális versenyképességét a nemzetközi viszonylatban. Amennyiben az európai szabványosítás együttesen a nemzetközi szabványügyi testületekkel összehangolt módon alkotja meg szabványait, nevezetesen a Nemzetközi Szabványügyi Szervezettel (ISO), a Nemzetközi Elektrotechnikai Bizottsággal (IEC) és a Nemzetközi Távközlési Egyesülettel (ITU) az európai ipari versenyképességet és az innovációt is elősegíti, közvetett módon támogatja az új, és jobb termékek vagy piacok fejlődését, és a jobb ellátási feltételek biztosítását, továbbá jelentős pozitív gazdasági hatásokat eredményez. A szabványok előirányzatként, fenntarthatják és javíthatják a minőséget, információt nyújthatnak, és biztosíthatják az interoperabilitást és kompatibilitást, ezzel növelve a biztonságot és az értéket a felhasználók, és más piaci szereplők számára. A műszaki szabványok jelentős hatást gyakorolhatnak a társadalom résztvevőire és fejlesztésük közvetett módon befolyásolja a

[148] Kovácsné Mozsár Lívia Alice, Biztonságos informatikai alkalmazás portfólió menedzselés, Óbudai Egyetem, 2018. "A COBIT (Control Objecitves for Information and Related Technology) egy keretrendszer arra, hogy a vezetőknek lehetősége legyen az előírásoknak való megfelelésnek. Alkalmazásával a szervezetek vezetőit segíti az üzleti céljaik elérésében, valamint az informatikai tevékenységek, költségek menedzselése is átláthatóvá válik."
[149] Z. Yazar, A qualitative risk analysis and management tool – CRAMM, SANS InfoSec Reading Room White Paper, 2002 - Citeseer
[150] Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről EGT-vonatkozású szöveg, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32012R1025, letöltés: 2019. november 24.
[151] Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról (EGT-vonatkozású szöveg), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32015L1535, letöltés: 2019. november 24.

polgárok biztonságát és gazdasági gyarapodását, az információs hálózatok hatékonyságát (információbiztonsági szabvány), a környezetünket (környezetvédelmi szabvány), a munkavállalók biztonságát és a munkavégzés körülményeit (minőségirányítási szabvány), a közlekedésünket (autóiparra vonatkozó szabvány). Ezáltal a polgárokat, a környezetet és a dolgozói érdekeket képviselő szervezeteket fokozott módon kell támogatni, és biztosítani kell a társadalmi érdekcsoportok szerepének növekedését és hozzájárulását a szabványok kidolgozása terén. A Római szerződésnek[152] megfelelően az uniós jogharmonizációs kötelezettségnek eleget kell tenni. Az Európai Unió több ezer, különböző, irányításhoz kapcsolható terület irányelvébe, utasításába vagy ajánlásába rögzítette az információbiztonságot, mint jogintézményt. Néhány példaként megemlíthető többek között, hogy az Európai Bizottság, mint az Európai Unió döntés-előkészítő, végrehajtó, döntéshozó, ellenőrző és képviseleti szerve már a 2001-ben, *Hálózat- és információbiztonság: javaslat egy európai politikai megközelítésre* című közleményében[153] hívta fel a figyelmet a hálózat- és információbiztonság növekvő jelentőségére. 2006-ban a biztonságos információs társadalomra irányuló stratégiát fogadták el[154], amelynek célja az európai hálózat- és információbiztonsági kultúra kialakítása volt. 2009-ben jelent meg a kritikus informatikai infrastruktúrák védelméről szóló bizottsági közlemény (CIIP)[155], amely Európa hálózati zavarokkal szembeni védelmével foglalkozik.[156] Az Európai Unió Tanács az információbiztonság témájú kérdésekkel kapcsolatos állásfoglalást fogadott el 2009-ben „*a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről*”. Az Európai Unió bár felismerte az információbiztonság tárgykörének fontosságát, korábban csupán közlemények, állásfoglalások szintjén foglalkozott ezzel a témával, a megelőzés, észlelés és elhárítás terén megvalósítandó feladatokat általános és kötelező jelleggel előíró jogszabályok elfogadására uniós szinten nem

[152] Római Szerződés (EGK), Az Európai Gazdasági Közösséget (EGK-t) létrehozó szerződés, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Axy0023, letöltés: 2018. június 7.
[153] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach, COM(2001) 298., https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52001DC0298, Letöltés: 2018. június 13.
[154] Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - “Dialogue, partnership and empowerment” {SEC(2006) 656}, COM(2006) 251., https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52006DC0251, Letöltés: 2018. június 13.
[155] COMMUNICATION FROM THE CO MMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMI TTEE OF THE REGIONS on Critical Information Infrastructure Protection , COM(2009) 149., https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF, Letöltés: 2018. június 13.
[156] Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE, a hálózat- és információbiztonságának az egész Unióban egységesen magas szintre vonatkozó intézkedésekről, COM/2013/048 final – 2013/0027 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013PC0048, Letöltés: 2018. június 13.

került sor. A biztonsági kérdések mellett a kibertámadások visszaszorítását is lényeges témának tekintették, ezt tükrözi *Az információs rendszerek elleni támadásokról* szóló 2005/222/IB tanácsi kerethatározat, amelynek célja a tagállami büntetőjogszabályok harmonizálása, a tagállamok igazságügyi és egyéb hatóságai közötti együttműködésének javítása érdekében, különösen a rendőrség és egyéb bűnüldözési szakszolgálatok terén. [157] [158] További, információbiztonság témaköréhez kapcsolódó szektorális szabályok megalkotására került sor, mint például *az elektronikus hírközlés*, 2009/136/EK irányelv, *a személyes adatok védelme*, 95/46/EK irányelv, *az általános adatvédelem, a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az adatok szabad áramlásáról* szóló rendelet és *a létfontosságú rendszerelemek védelme*, 2008/114/EK irányelv. Az irányelvek[159] olyan európai uniós jogi aktusok, amelyek az elérendő célok tekintetében kötelezik a tagállamokat, de az általános cél megvalósításának konkrét formáját, a megfelelő eljárásokat és eszközöket a tagállamok maguk választják meg. A tagállamoknak kötelességük, hogy az irányelvben foglaltak meghatározott időn belül nemzeti jogszabályaikban meghatározásra kerüljenek, azaz jogszabályi szinten rögzíteni kell az előírásokat. További stratégiai döntés, az Európai Bizottság által 2010. év májusában megalkotott Európai Digitális Menetrend*[160]*. A stratégia célja általánosságban a nagy sebességű és szupergyors internetre és interoperábilis alkalmazásokra épülő egységes digitális piac, amely által fenntartható gazdasági és szociális előnyöket teremtsen az EU tagállamok számára. Az európai digitális menetrend az „*Európa 2020*” stratégia kezdeményezéseinek része, amelynek célja az információs és kommunikációs technológiák (IKT-k) alkalmazásának kulcsfontosságú szerepének kijelölése az Európa 2020-ra kitűzött céljainak sikeres megvalósításában.

2.4.6.1. INFORMÁCIÓBIZTONSÁGI SZABÁLYOK NÉMETORSZÁGBAN

Németország technikai és szabályozás terén is vezetőnek tekinthető az Európai Uniós tagállamok között, ezért technikai fejlettségük és szabályok alkalmazása mintaként szolgálhat egyes, kevésbé fejlett tagállamok számára. Ebben a fejezetben a témával kapcsolatos néhány német jelentősebb mérföldkőre szeretném felhívni a figyelmet. Németország a fejlett ipari, gazdasági és társadalmi helyzetüknél fogva igyekezett mielőbb alkalmazni az IT lehetőségeket

[157] Bodó Attila Pál, Információbiztonsági jogi ismeretek vezetőknek, Nemzeti Közszolgálati Egyetem, Budapest, 2014
[158] A TANÁCS 2005/222/IB KERETHATÁROZATA, (2005. február 24.), az információs rendszerek elleni támadásokról
[159] Európai uniós irányelvek, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Al14527, Letöltés: 2018. június 11.
[160] Az európai digitális menetrend, http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=COM:2010:0245:FIN, letöltés: 2021. december 4.

mind az iparban, a közszférában, a gazdasági és a lakossági szférában egyarán. Az 1983. évi internet bevezetése európai viszonylatban is korainak tekinthető, bár az egy évvel később megjelent e-mail rendszerük[161] kevésbé tud versenyezni az amerikai e-mail rendszer bevezetésével és elterjedésével, mégis elmondható, hogy a német ICT[162] piac a legnagyobb Európában[163] és világ szinten is a legelsők közt szerepel. A széles körben elterjedt ICT nemcsak az informatikai fejlődést, hanem potenciális támadási célpontot is jelent a szintén dinamikusan fejlődő cracker réteg számára, ezért a német virtuális világ védelmi és szabályozási stratégiája és az intézkedések is folyamatos fejlődést mutatnak. Az információs technológiák mindenütt jelen vannak és megváltoztatják életmódunkat és munkánkat. A digitalizálás példátlan új szabadságokat hoz nekünk, új lehetőségeket teremt a kapcsolattartásra és elősegíti a társadalmi fejlődést. A német Szövetségi Belügyminisztérium Németországra vonatkozó digitális politikájának célja, hogy minél több ember számára megnyissa az Internet adta sokszínű lehetőségeket, és emellett előtérbe helyezi az internetes kockázatok radikális csökkentését, és minimalizálását. A szabad virtuális kommunikáció azonban szabályozás nélkül nem működik, mivel a szabadság gyakorlására is szabályokra van szükség. A német *Digitális Menetrend 2014-2017* dokumentáció rögzítésekor hét olyan területet fogalmaztak meg, ahol a szükséges intézkedéseket végre kell hajtani, amely szerint a következők lehetnek a gyors internethálózat hatékony kiépítésének technikai és szabályozási hátterének megvalósítása, a digitális gazdasági és digitális munkahelyek megteremtése és fejlesztése, az innovatív kormányzás, a közszolgáltatás digitális transzformációja (például: a „*2020 Digitális Közigazgatás*” projekt), a lakossági digitális környezet kiépítése, az ország innovatív képességének fenntartása, mindez az oktatás, K+F, kultúra és média területein, a tudásbázis támogatásával, a biztonság és a védelem az online térben, az összhang megteremtése nemzeti, nemzetközi és Uniós szinten. A német Digitális Menetrend felülvizsgálatát követően meghatározták a digitalizáció következő irányvonalát, amelyet a német Szövetségi Gazdasági és Energetikai Minisztérium adott ki „*Digitális Stratégia 2025*” címmel. A gazdasági mutatók szerint az ICT szektor bevétele és a munkahelyek száma is jelentősen növekedett.[164] Maga a stratégia egy tíz pontból álló program, amelyben megtalálható az 1 GB-os optikai országos hálózat kiépítése 2025 év végéig, a

[161] Das waren die Roots: Wie das Internet nach Deutschland kam, https://www.heise.de/newsticker/meldung/Das-waren-die-Roots-Wie-das-Internet-nach-Deutschland-kam-120535.html, letöltés: 2019. december 3.
[162] Information and Communication Technologies
[163] The 2018 PREDICT Key Facts Report, JRC Technical report (by the Joint Research Centre), 2018., https://publications.jrc.ec.europa.eu/repository/bitstream/JRC112019/jrc112019_2018_predict_key_facts_report.pdf, letöltés: 2019. december 3.
[164] Digitális Stratégia 2025

„*startup*" vállalkozások támogatása, a szabályozási keretek kialakításával a digitális egységes piac létrehozása nemzeti és Uniós szinten, az okoshálózatok támogatása a gazdaságilag jelentős területeken, különösen az energiaszektorban, a közlekedésben, az egészségügyben, az oktatásban és a közigazgatásban, az adatbiztonság támogatása, a digitalizáció támogatása a kis- és középvállalatok tekintetében, új üzleti modellek használatával (*Digitális Beruházási Program*), az Ipar 4.0 technológiák támogatása és alkalmazása az ipari környezetben, a digitális K+F tevékenységek erősítése, kutatási költségek finanszírozásának támogatása, a digitális írástudás és szakemberpótlás, szakképzés támogatása, és a digitális ügynökségek felállítása (*Szövetségi Hálózati Ügynökség*). A németországi információbiztonsági és adatvédelmi felülvizsgálatok következtében megalkotott irányelvek alapján, 2018-ban elsődleges digitális menetrendre vonatkozó témák merülnek fel, mint például az információs hálózat legmagasabb szintű biztonságának igénye - rendezett és biztonságos keretfeltételek a digitális világ számára, az állampolgárokat és a gazdaságot kiszolgáló modern, digitális adminisztráció[165], továbbá erős és tudatos az a civil társadalom megteremtése[166], valamint legyenek elérhetőek a digitalizáció etikai iránymutatásai és korszerű az adatpolitika – mindez új technológiák alkalmazásának lehetőségével és a kockázatok korlátozásával.[167] A német Digitális Menetrend – amely hűen igazodott az Európai Digitális Menetrendhez – következtében új kiadásra került az IT biztonsági törvény *IT-Sicherheitsgesetz 2.0* névvel. Az új kiadás mottója a több védelem, a több biztonság és a több információ. A törvénybe rögzítésre került az, hogy a kibertámadások veszélye továbbra is változatlan marad, mivel a támadások dinamikusabbá, változatosabbá és egyre profibbá válnak. A fenyegetésből származó kockázatok csökkentését a szakemberek és a jogalkotó az adat- és infrastruktúra-biztonság jelentős megerősítésében látják. A törvény kiadásával kibővítették a BSI[168] lehetőségeit a szövetségi IT rendszerek védelmére. A BSI az információbiztonság megvalósításának egyik alapja Németországban. Feladata az, hogy gyorsan és megfelelően kezelje a kibertér által jelentett veszélyeket. Az európai és a német digitális menetrend nemcsak technológiai fejlesztést, hanem humánerőforrás bővítést tűzött ki céljául az IT szakterületen. A BSI-nek képesnek kell lennie arra, hogy észlelje és elkerülje a kormányzati rendszerek elleni támadásokat. Ennek elérése érdekében növeli az adattárolási és –feldolgozási lehetőségeket. Az IT biztonsági törvény második kiadásának alkalmazásával

[165] hatékony, megbízható és polgárbarát, kivitelezését eljárások segítik
[166] digitalizálás, tanácsadás és támogatás nyújtása a felhasználók számára
[167] Die Digitale Agenda des BMI, Bundesministerium des Innern, Für Bau und Heima, Berlin, 2019., https://www.bmi.bund.de, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2019/03/digitale-agenda.html letöltés: 2022. július 18.
[168] Bundesamt für Sicherheit in der Informationstechnik

többek között a német polgárok információbiztonsági tudatosságát kívánták növelni, mindezt informatikai tanácsadó központok kiépítésével, továbbá a törvényi követelményeket kiterjesztették az informatikai eszközöket, alkatrészeket előállító gyártók tevékenységére is, akiknek publikálni kell a minőségi tanúsítvány az adott eszköz kiadása előtt. A rendelkezésekkel szigorították a számítógépes büntetőjogi rendelkezéseket, valamint létrehozták a számítógépes bűncselekmények és bűncselekményre utaló események bejelentési lehetőségét kezelő úgynevezett eseménykezelő központokat. A törvény lehetőséget teremtett a Nemzeti Kibervédelmi Központ[169] feladatának kibővítésére is. Természetesen a feladat a törvényalkotásnál és az egyes intézetek felállításánál kibővítésénél nem állt meg. A német szövetségi kabinet 2018. évében létrehozott egy új információbiztonsági innovációs ügynökséget[170] is, tekintettel arra, hogy szükségessé vált a kiberbiztonsági projektek technológiai fejlesztésének tervezése és finanszírozása. A német Digitális Menetrendhez kapcsolódik az Online hozzáférési törvény[171], amely a polgárok, vállalkozások és hivatalok digitális adminisztratív feladatait segíti elő, a papír alapú adminisztráció minimalizálásával. A német szövetségi kormány a *Digitális adminisztráció 2020*[172] programmal létrehozta a közigazgatás digitalizálásának keretfeltételeit is. A dokumentáció értelmében a közigazgatás rugalmasságát, valamint a német szövetségi információs technológia finanszírozhatóságát, és IT biztonságát hosszú távon is biztosítani kell. A program célja tehát az állampolgárok és a vállalkozások számára nyújtott adminisztratív szolgáltatások digitalizálása. A program keretében összesen 575 digitalizálandó szolgáltatást azonosítottak[173]. A kiadott OZG katalógusban az 575 szolgáltatást 35 élet- és 17 üzleti helyzethez csoportosítják, valamint 14 felügyelt tematikus területhez rendelik, mint például *Család és gyermek* vagy a *Vállalatirányítás és fejlesztés* témákhoz. A projekt részeként a különösen fontos szolgáltatások tekintetében 2019. évtől online, digitalizáló laboratóriumok létrehozását tervezték a polgárok és a vállalkozások részére. Lényegében az OZG programjainak alkalmazásával paradigmaváltás zajlik, ahol a központi szerepbe a felhasználókat helyezték, és a meglévő korlátozásokat általános feltételekként határozza meg. A dokumentum szerint a digitális

[169] Nationale Cyber-Abwehrzentrum
[170] Agentur für Innovation in der Cybersicherheit
[171] Umsetzung des Onlinezugangsgesetzes (OZG), hatályba lépés: 2017. nyara
[172] Digitale Verwaltung 2020
[173] Megjegyzés: A szolgáltatások között megtalálható a 115 „1. típusú szolgáltatás", amely szerint a szabályozási és végrehajtási hatáskör a szövetségi kormánynál van, továbbá a 370 „2/3 típusú szolgáltatás", amely szerint a szabályozási kompetencia szövetségi szinten és végrehajtási kompetencia tartományokban és önkormányzatokban van, valamint a 90 „4/5 típusú szolgáltatás" a szabályozási és végrehajtási kompetenciák a tartományok és az önkormányzatok számára.

adminisztrációs szolgáltatások tervezésére és kidolgozására vonatkozó iránymutatások előkészítik az utat a felhasználó-orientált megoldásokhoz. A digitalizáció szabályozása, és a vonatkozó intézkedések végrehajtásának elősegítése érdekében gyakorlati iránymutató rendszert is létrehoztak.[174] Az online hozzáférési törvény kimondja, hogy a szövetségi kormánynak és a tartományoknak 2022-ig digitálisan közigazgatási portálokon keresztül kell biztosítaniuk minden közigazgatási szolgáltatást, és ezen kívül össze kell kapcsolniuk a portálokat. A cél a közigazgatási portálhálózat kialakítása. Az Európai Unió által előirányzott IT rendszerek interoperabilitásának kialakítása immár elvárt feladat, így a portálok mögött létrehozott IT rendszereket úgy kell megalkotni vagy módosítani, hogy adatstruktúrájuk kompatibilis, szinkronizálható, szemantikai és szintaktikai szabályokat is teljesítő komplex rendszerré válhasson. A rendelkezés rögzíti, hogy a portálhálózatban használt informatikai komponensek és a portálhálózathoz való kapcsolódás tekintetében az informatikai biztonság biztosításához szükséges műszaki, kommunikációs szabványokat. A rendeletben meghatározott szabványoknak való megfelelés minden német szervre, amely a közigazgatási adminisztratív szolgáltatásokat használja, kötelező érvényű. A szövetségi adatvédelmi törvény vonatkozó részeit minden esetben figyelembe kell venni. Az informatikai biztonsági előírások betartása kötelező minden résztvevő jogi és természetes személy számára, aki az IT komponenseket használja. A rendelkezés Németország egész területére vonatkozik, az összes tartományban egységesen kell alkalmazni. A felhasználók személyazonosságának meghatározása és elektronikus nyilvántartása[175] érdekében a felhasználói regisztrációkor rögzítésre kerülnek a felhasználói személyes adatok (név, cím, születési idő, személyi azonosító) és jogi személy esetében, a társaság egyértelmű azonosítására vonatkozó adatok (cégnév, regisztrációs szám, székhely, cím, képviseletei tagok neve). A törvény lehetőséget ad arra, hogy az illetékes szervezetek a regisztrációhoz és a nyilvántartáshoz szükséges adatokat a kapcsolattartás érdekében és az elDAS rendelettel összhangban gyűjthessék. A felhasználói fiókban, a felhasználó beleegyezésével, az adminisztratív folyamatokkal, valamint a felhasználói fiókon belüli állapot- és eljárási információkkal kapcsolatos elektronikus dokumentumok tárolhatók és kezelhetők. Az elektronikus azonosítás az azonosító adatok egyetlen lekérdezésével hajtható végre. A felhasználó beleegyezésével megengedett az azonosító adatok állandó tárolása, továbbítása és felhasználása az adminisztratív teljesítésért felelős hatóság számára. Állandó

[174] Leitfaden zum Digitalisierungsprogramm des IT-Planungsrates, 2019., https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Digitalisierungsprogramm/DigPro_Leitfaden.html?nn=11113802, letöltés: 2019. december 4.

[175] Gesetz zur Förderung des elektronischen identitätsnachweises, 2017., 2021., https://www.bgbl.de/xaver/bgbl, letöltés: 2022. július 19..

tárolás esetén a felhasználónak mindig lehetősége van arra, hogy a felhasználói fiókot és az összes tárolt adatot egymástól függetlenül törölni. A közigazgatási szolgáltatás kezeléséért felelős hatóság[176] a felhasználó beleegyezésével egyedi esetekben elektronikus úton lekérdezheti a felhasználói azonosításához szükséges adatokat a felhasználói fiókért felelős irodából. [177] A digitalizálás olyan gazdasági, társadalomi és adminisztrációs változási folyamatot indít el, amellyel vélhetően a polgárok és a gazdasági társaságok számára nyújtott közszolgáltatások egyszerűbbek, hozzáférhetők és ugyanakkor hatékonyabbak lehetnek[178].[179] A *Digitális Stratégia 2025*, a német Szövetségi Gazdasági és Energetikai Minisztérium által 2016. évben kiadott, Németország digitalizációval kapcsolatos hivatalos iránymutatást fogalmaz meg. A dokumentum célja, hogy a nemzetközi IT és IKT fejlődés egyik vezető országává váljon, amit infrastrukturális fejlesztésekkel, a befektetések támogatásával és innovatív fejlesztésekkel érnek el. A kormányzati értékelések alapján megállapítható, hogy a stratégia kiadását követő első év szerint kimutatható mértékben növekedtek a szektor bevételei, az infokommunikációs szektorban pedig több ezer új munkahelyet sikerült létesíteni.[180] A stratégia tíz pontból álló program, amely keretében 2025-re 1 GB-os országos optikai hálózat létrehozását, „*startup"* vállalkozások, okoshálózatok támogatását legfőképp az energiaszektor, a közlekedés, az egészségügy, az oktatás, a közigazgatás területein, az adatbiztonság erősítését és az információs autonómia kialakítását, a kis- és a középvállalatok számára új üzleti modell megalkotását, az Ipar 4.0 megoldások alkalmazását, valamint a digitális K+F ösztönzését tűzte ki céljául. A stratégia megvalósítását nemzetközi együttműködések, fórumok is segítették az elmúlt években. A nemzetközi együttműködés eredményeként Németországban került megrendezésre 2019-ben az Internet Governance Forum (IGF) az Egyesült Nemzetek Szervezetének éves nyílt vitafóruma, ahol az internet legfontosabb jogi, politikai, társadalmi és technikai kérdéseiről tartottak beszámolókat. A konferencia célja, a helyi és regionális internetes közösség, köztük a piaci szereplők, a technikai támogató szervezetek, a kormányzati

[176] die Abwicklung einer Verwaltungsleistung zuständige Behörde
[177] Umsetzung des Onlinezugangsgesetzes (OZG), Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen, http://www.gesetze-im-internet.de/ozg/ ,letöltés: 2022. július 19.
[178] Onlinezugangsgesetz (OZG), Die Interaktion zwischen Bürgerinnen, Bürgern und Unternehmen mit der Verwaltung soll in Zukunft deutlich schneller, effizienter und nutzerfreundlicher werden. https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html, letöltés: 2022. július 19.
[179] A digitális program célképe (Német Szövetségi Belügyminisztérium), Zielbild des Digitalisierungsprogramms, Quelle: Bundesministerium des Innern, für Bau und Heimat, 2019., Digitale Verwaltung: nutzerorientiert und modern Digitalisierungsprogramm zur Umsetzung des OZG: Blaupausen für die Verwaltungsdigitalisierung, 2022. július 19.
[180] Molnár Dóra: Kiberbiztonság Németországban – pillanatkép a német digitális térről, Nemzet és Biztonság 2018/1.

tisztviselők, az oktatók és a fiatal tehetségek bevonzása. A találkozókat a nemzetközi információcsere és inspiráció céljából szervezik. Németország első alkalommal 2019-ben fogadta a Fórum résztvevőit, ahol általában több, mint 160 ország 5000 résztvevővel képviselteti magát.[181] Az IGF első ülését 2006. évben Athénban, Görögországban tartották. Az ülés átfogó témája az internetes fejlesztés irányítása volt. A napirendet öt széles témára osztották fel, így a nyitottság (a véleménynyilvánítás szabadsága, az információk, ötletek és tudás szabad áramlása), a biztonság (bizalom megteremtése együttműködés révén), a sokféleség (a többnyelvűség és a helyi tartalom előmozdítása), a hozzáférés (Internet-kapcsolat, politika és költségek), vagy a kapacitásépítés prioritása. A 2018. évi Párizsban megrendezett IGF már erőteljesebb témáknak adott otthont, amely az internet szabályozására, valamint az internetes támadások, gyűlöletbeszéd és más számítógépes fenyegetések elleni küzdelemre irányult. Nyolc téma alkotta a 2018. évi menetrend gerincét. A témák között szerepelt a kiberbiztonság, bizalom és adatvédelem, a fejlesztési, innovációs és gazdasági kérdések, a digitális integráció és hozzáférhetőség, az emberi jogok (nemek és az ifjúság), a feltörekvő technológiák, az internetes kormányzás kialakítása, a média és a tartalom, valamint a műszaki és működési kérdések. Az IGF 2022 évi fórumán kiemelt témát kaptak az adatvédelmi, kiberbiztonsági és mesterséges intelligencia kérdései[182].

2.4.6.2. ADATBIZTONSÁGI SZABÁLYOK NÉMETORSZÁGBAN

Németországban az adatvédelmet különböző rendeletekkel szabályozzák.[183] Az általános szabályok közül különösen az általános adatvédelmi rendeletet (DS-GVO), a német szövetségi adatvédelmi törvényt (BDSG)[184] és az adatvédelmi és információszabadság törvényét (HDSIG)[185] kell megemlíteni. Számos más német törvény tartalmaz adatvédelmi rendelkezéseket is, mint például SGB[186], vagy a távközlési törvény (TKG)[187] és a médiára vonatkozó törvény (TMG)[188]. A német szövetségi adatvédelmi törvény a BDSG 2018. évtől hatályos változatát az EU adatvédelmi adaptációs és végrehajtási törvény (DSAnpUG-EU)[189]

[181] Bundesministerium Für Wirtschaft Und Klimaschutz, Das Internet Governance Forum, https://www.bmwi.de/Redaktion/DE/Videos/2019/20191129-igf-2019-tag4.html, letöltés: 2022. július 19.
[182] Internet Governance Forum (IGF), https://www.intgovforum.org/en/content/igf-2022-themes, letöltés: 2022. július 19.
[183] DS-GVO, Datenschutz-Grundverordnung, https://dsgvo-gesetz.de/, letöltés: 2022. július 29.
[184] BDSG, Bundesdatenschutzgesetz, https://dsgvo-gesetz.de/bdsg/, letöltés: 2022. július 29.
[185] HDSIG, Gesetzestext Hessisches Datenschutz- und Informationsfreiheitsgesetz, https://datenschutz.hessen.de/infothek/gesetze, https://dsgvo-gesetz.de/hdsig/, letöltés: 2022. július 29.
[186] SGB, Sozialgesetzbuch
[187] TKG, Telekommunikationsgesetz
[188] TMG, Telemediengesetz
[189] DSAnpUG-EU, Datenschutz-Anpassungs- und Umsetzungsgesetz EU

részeként fogadták el. A BDSG új verziója 2018. május 25-től alkalmazandó az általános adatvédelmi rendelettel (DS-GVO). Az adatvédelmi törvény módosítása, a második DSAnpUG-EU 2019. november 26-án lépett hatályba. A törvény hatálya kiterjed mind a szövetségi kormány hatóságaira, a tartományok állami intézményeire és ügynökségeire, mind pedig a nem állami szervezetek a személyes adatainak kezelésére, feldolgozására, kivéve, ha az személyes vagy családi tevékenységre irányul. A törvény hűen követi a GDPR szabályait is, amely négy részből áll, tehát a közös rendelkezések, az általános adatvédelmi rendelet (GDPR) 2. cikk szerinti az adatfeldolgozás végrehajtási rendelkezései[190], a 2016/680 EU irányelv 1. cikk (1) bekezdésében említett célokra vonatkozó adatfeldolgozás rendelkezései[191], valamint az általános adatvédelmi rendelet és az irányelv által nem szabályozott tevékenységekkel kapcsolatos feldolgozásra vonatkozó különös rendelkezések. A közös rendelkezések részei többek között a hatályosság és definíciók meghatározása, a személyes adatok feldolgozásának jogalapja (a személyes adatok állami hatóságok általi feldolgozása és a nyilvános terek video-megfigyelése), a hatóság által kinevezett adatvédelmi tisztviselő joga és feladata, valamint kijelölésére, pozíciójára vonatkozó előírások, az adatvédelemért és az információszabadságért felelős szövetségi biztos, mint hivatalos személy jogai, feladatai és hatásköre, ezen kívül függetlensége, kinevezése és hivatali időtartama, képviselet az Európai Adatvédelmi Testületben, az egyablakos ügyintézés, a szövetségi és állami felügyeleti hatóságok közötti együttműködés az Európai Unió ügyeiben, valamint jogorvoslatok, igazságügyi védelem. Az (EU) 2016/679 rendelet 2. cikkében említett célokra vonatkozó feldolgozás végrehajtási rendelkezései a személyes adatok feldolgozásának jogalapjára vonatkozó szabályozás érinti a személyes adatok különleges kategóriáinak feldolgozását és egyéb célokra történő feldolgozást, valamint a hatóságok általi adattovábbítást, továbbá a különleges adatfeldolgozási helyzeteket (úgymint a foglalkoztatási célokra, tudományos vagy történelmi kutatási és statisztikai célokra, közérdekű archiválási célokra vonatkozókat), a szükséges jogokat titoktartási kötelezettség esetén, valamint az érintettek jogait, az információszolgáltatási kötelezettséget és eseteit, tájékoztatási kötelezettséget (ha a személyes adatokat nem az érintett adta meg), az érintett

[190] A GDPR (2016/679 EU rendelet) 2. cikkében említett célokra vonatkozó, adatfeldolgozás végrehajtási rendelkezései, amely szerint alkalmazni kell a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

[191] A GDPR (EU) 2016/680 irányelv 1. cikkének (1) bekezdésében említett célokra történő, adatfeldolgozásra vonatkozó rendelkezések szerint szabályokat állapít meg a természetes személyek védelmére a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében

személy információhoz való jogát, a törlés jogát, automatizált eseményekhez kapcsolódó információhoz való jogát (profilozás), az adatkezelők és az adatfeldolgozók felelősségét, és magánszervezetek adatvédelmi tisztviselőinek jogait és feladatait. A második részhez hozzátartozik a felügyeleti hatóság a nem állami testületek által végzett adatfeldolgozása, a szankciók, úgymint a bírság és a büntetőeljárás szabályainak alkalmazása vagy a büntetőjogi rendelkezések és közigazgatási bűncselekmények kezelése és az esetleges jogorvoslati kérdések kezelése.

2.4.7. AZ INFORMÁCIÓBIZTONSÁG HAZAI KÖZIGAZGATÁSI SZABÁLYOZÁSI RENDSZERE

Az információbiztonság helyzete és állapota magyarországi közigazgatási intézményekben megfelelőnek tekinthető. Ez köszönhető a bevezetett és alkalmazott jogszabályi előírásnak, valamint a tudatosítás rendszerének. A közigazgatási szabályozások célja, hogy az információs rendszerek biztonságát és az alkalmazotti biztonságtudatosságot is növeljék, az információs rendszereket ért biztonsági eseményeket megelőzzék, vagy hatásukat csökkentsék, ezáltal a biztonsági szintet emeljék. Ugyanakkor az informatikai biztonsági incidensek sokszor informatikai hiányosságokra, illetve a biztonságtudatosság hiányára vezethetők vissza. Bár sok esetben a felmérések és interjúk megfelelő információbiztonsági állapotra utalnak, mégis a bekövetkezett incidensek informatikai ismeretek hiányosságaira utal, ami kockázatot jelent a közigazgatás minden szintjén. A kockázatok vizsgálata nemcsak az információs eszközök tulajdonságára, állapotára vonatkozik. Figyelembe kell venni az adott intézményt is, mivel a kockázatok a szervezeteken belül a felhasználók tudásszintjével, és jogosultságaik mértékével arányosak. Az információbiztonság a közigazgatási információs rendszerben jelen korunk vívmánya. Az elmúlt évtizedek történései határozzák meg napjaink intézkedéseit is. Magyarország Országgyűlése 2013. április 15-én fogadta el az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényt (Ibtv.). A törvény része annak az információbiztonsági stratégiának, amely kezelni kívánja a modern információs társadalmat, a digitális infrastruktúrát, valamint a kibertérből származó és a hazai kiberteret ért fenyegetéseket és a hazai információs infrastruktúra sérülékenységeit. Mindezt a nemzetközi előírások, ajánlások és trendek, valamint a hazai rendelkezések és igények is alátámasztják. Az Ibtv. számos új jogintézmény fogalmát pontosítja és új követelményi rendszer támaszt a biztonságért

felelős szervezetekkel szemben.[192] A jogszabály által olyan speciális információbiztonsági programokat, stratégiákat és adott esetben a jogszabályi megfelelés szerinti infrastruktúra fejlesztési terveket kell készíteni, és intézkedéseket kell végrehajtani, amely összhangban van egyben az intézményi stratégiával, valamint az információs technológiát koordináló szervezet munkafolyamataival, fejlesztési igényével és információbiztonsági követelményrendszerrel. A törvényben meghatározott célokat és feladatokat rögzítettek, amelyek végrehajtását részterületenként határozták meg. A feladat végrehajtásához képzési rendszert is rendeltek jogszabályi támogatással.[193] További Európai Uniós rendelkezések közé tartozik a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló Európa Parlament és Tanács által elfogadott (EU) 2016/1148 számú irányelvnek (NIS irányelv)[194] európai szintű végrehajtása és magyar jogrendbe történő átültetése. A rendelkezések 2018. május 10. napján hatályba léptek. Az információs rendszerek megbízható, folyamatos működésére alapvető gazdasági és társadalmi tevékenységek támaszkodhatnak. Az erre épülő célokat, illetve a kibertéri működés biztonságát és „üzletmenetfolytonosságát" támogatják az illetékes hatóságok és a közigazgatási szervek. Az Európai Uniós rendelet előírja az államigazgatási és közigazgatási szférában, valamint ezen szervezetekhez tartozó intézményekben a hálózati és információs rendszerek kockázatokkal arányos védelmét és az alkalmazandó biztonsági elemeket. A tudományos kutatásokat nemcsak az információs technológia és az információs rendszer szempontjából kell elemezni, hanem a vizsgálat része maga az információs társadalom, így a felhasználói kör is. Jellemző, hogy a felhasználók egyre újabb eszközöket, információs szolgáltatásokat vesznek igénybe az intézményekben és a magánszférában egyaránt. A népszerű készülékek, így az okostelefonok, laptopok, táblagépek megkönnyítik az életünket. Az új típusú információs eszközökhöz azonban több különböző szolgáltatás szükséges, amiben személyes információkat és intézményi adatokat szinkronizálják, akár néhány perces gyakorisággal. A kényelmi megoldások nagyon könnyen megszokhatók, de következménnyel is jár. A magán és a munkavégzéssel összefüggő adatok keverednek, a biztonságuk sérülhet, és illetéktelenek

[192] Illéssy Miklós, Nemeslaki András, Som Zoltán, Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs Társadalom, Társadalomtudományi Folyóirat, 14 (1). pp. 52-73. ISSN 1587-8694, 2014.

[193] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet

[194] Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148, letöltés: 2019. június 1.

kezébe kerülhet. A világhálón az elérhető szolgáltatások fejlődésével, a közösségi funkciók is rendkívüli gyorsasággal terjednek. A közösségi funkciók használatával, annak összefüggésével a biztonsági kockázatok számossága és a hatásuk mértéke is nő. Manapság sok esetben természetesnek tartják a személyes adatok megadását nyilvános weboldalakon, a közösségi médiában. Olyan adatokat, amelyet korábban csak közeli ismerőseinkkel, munkatársainkkal osztottak meg. Egyes közösségi szolgáltatások világszintű népszerűségével és alkalmazásával, gigantikus felhasználói és adatrekord száma csak megbecsülhető, így szintén csak becsülhető, hogy milyen mértékű lehet a kár, egy szoftverhiba, vírus vagy kártékony program károkozása folytán. A közigazgatáson belül az intézményi információbiztonsági szabályozás kialakítása és alkalmazása szükséges, amelyhez hozzájárul a szakmai irányítás és felügyeleti intézményrendszer kialakítása. A szakmai továbbképzések és a vonatkozó információs fórumok támogatják a szakemberek együttműködését és szakmai fejlődését (Networkshop, Adatvédelmi tisztviselők éves konferenciája, HBONE). További feladat a kezdeményezések támogatása és tudatosítása, mind intézményi, mind szervezeti szinten egyaránt. Sajnos, a szükséges biztonsági szint csak évek alatt érhető el, de a jelenlegi jogszabályi rendszer lehetővé teszi a fokozatos fejlődést, a szigorúbb követelményeket, figyelembe véve az adatvédelem prioritását.[195]

2.4.7.1. INFORMÁCIÓBIZTONSÁGI POLITIKA ÉS IRÁNYELVEK

Az információbiztonsági biztonságpolitika célja, hogy az adott intézmény szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának biztosítása érdekében követendő irányelvekre. Az irányelvek figyelembevételével meghatározható az informatikai rendszerek biztonsági osztályba sorolása, kidolgozható a konkrét, rendszer szintű informatikai biztonsági szabályozás, amely meghatározza a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez a szükséges alapelveket és követelményeket. Az intézmény vezetősége az információbiztonsági biztonságpolitika elfogadásával támogatja az információbiztonság céljait és alapelveit, a működési stratégiával és a célokkal összhangban. Az informatikai rendszerek biztonsági, az intézmény működéséhez igazított kategóriáit az intézményi szabályzatában részletezi. A biztonságos használatra és üzemeltetésre vonatkozó felhasználói előírásokat a vonatkozó informatikai vagy üzemeltetői szabályzat tartalmazza. Az

[195] Horváth Gergely Krisztián, Kormányzati Informatikai Fejlesztési Ügynökség: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, , Budapest, 2013

intézmény szervezeti egységei által kezelt adatok, információk védelmét bizalmasság, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából úgy kell megvalósítani, hogy az informatikai rendszernek és környezetének védelme folytonos, teljes körű, zárt és a kockázatokkal arányos legyen, valamint megvalósuljon a zárt szabályozási ciklus. Az információbiztonsági ajánlások, informatikai rendelkezések és törvények figyelembe vételével a lehetséges általános, információbiztonsági irányelvek különösen a hitelesség biztosítása, a bizalmasság biztosítása, a sértetlenség biztosítása, a rendelkezésre állás, a biztonsági osztályba sorolás és a működőképesség fenntartása. Az általános irányelvek figyelembevételével további alapelvek alakíthatók, úgymint a teljes körűség[196], a zártság[197], a kockázatarányosság[198], a folytonosság[199], a zárt szabályozási ciklus alapelve[200], a differenciált védelem[201], a fenntarthatóság[202]. a kockázatelemzés, engedélyezés[203]. A kockázatokat lehetőség szerint minimalizálni kell. Minden felhasználóban tudatosítani kell, hogy teljes körű védelem és biztonság nincs, és ezzel összefüggésben a maradvány kockázatot az intézmény illetékes szervezeti egysége tudatosan vállalja, és elkészíti az intézmény informatikai, információbiztonsági üzletmenet folytonossági tervét és elemzését. Az elemzés része a kockázatspecifikáció. A specifikáció tartalmazza a kockázatfelmérés módszertant, kockázatok azonosítását (potenciális fenyegetettségek számbavétele), a katasztrófabekövetkezés valószínűségének, jellegének (hirtelen, fokozatos) és lefolyása időtartamának meghatározását. Az elemzés során a következő dokumentumok kidolgozása elengedhetetlen: a vagyonleltár, a helyzetelemzés, a kockázatelemzés és specifikáció, a kockázatkezelés, és hatáselemzés, valamint az intézkedési tervek. A vagyonleltár tartalmazza a vagyonelemek felmérését (megnevezése, mennyisége, fellelhetősége, hozzáférők száma, biztonsági besorolása,

[196] A védelmet fizikai, logikai és adminisztratív vonatkozásban egyaránt érvényesíteni kell.
[197] A védelem zártságát akkor lehet biztosítani, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedések megvalósulnak.
[198] A védelem akkor kockázatarányos, ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak.
[199] Az informatikai rendszerek bevezetése és fejlesztése során kialakított védelmi konfigurációkat a rendszerből való kivonásig folyamatosan biztosítani kell, mégpedig a rendszeres ellenőrzéssel és biztonsági intézkedésekkel.
[200] A zárt szabályozási ciklus úgy érvényesíthető, hogy az adminisztratív védelemben biztosítani kell: a szabályozás-, érvényesítés-, ellenőrzés-, szankcionálás folyamatát és a ciklikus folyamatosságát.
[201] Az informatikai rendszerek védelmét az általuk kezelt adatok biztonsági osztályba sorolására kell alapozni.
[202] Létfontosságú, hogy a fokozott biztonsági kategóriájú informatikai rendszereket olyan környezetben kell telepíteni és működtetni, amelyben az adatok és az adatfeldolgozás bizalmassága, sértetlensége, rendelkezésre állása és auditálhatósága egyaránt magas szinten garantált. Az információbiztonsági ellenőrzésekről minden esetben jegyzőkönyvet kell felvenni.
[203] Megfelelő felhasználói felhatalmazás, jogosítvány, engedély kibocsátás és jogosultság kibocsátás. A felhasználói jogosultságok természetes személyhez kötöttek és nem átruházhatók. Rosszhiszemű felhasználásnak tekintendő, ha a felhasználó a jogosultságát meghaladó műveleteket szándékosan kezdeményez, illetve jogosultságát megkísérli módosítani.

kezelésének felelőse, szabályozása, hozzáférési teszt dátuma), a vagyonelem-kategóriák szerinti csoportosítást, valamint a vagyonelemek fenyegetéseinek és sebezhetőségeinek rögzítését. A kockázatelemzés és specifikáció tartalmazhatja különösen az esetleges incidens mérhető hatását az adott Intézményre, a lehetséges fenyegetések bekövetkezésének valószínűségét, kockázatának számítását (hatás és valószínűség szorzata), valamint a lehetséges incidens megelőzésére vonatkozó szükséges döntést és kockázati érték meghatározását. Az információbiztonsági politika alapelvei alapján elkészítendő, kapcsolódó dokumentum lehet, különösen az adatvédelmi és adattovábbítási szabályzat, az informatikai szabályzat, a információbiztonsági szabályzat, az információbiztonsági üzletmenetfolytonossági terv, az informatikai üzemeltetési és szolgáltatói rendelkezések, az elektronikus dokumentumok biztonsági adatmentésének szabályai, valamint az információbiztonsági fejlesztési terv.

2.4.7.2. INFORMÁCIÓBIZTONSÁGI AJÁNLÁSOK

A hazai hagyományokhoz hűen Magyarország ismét élenjárt az újdonságok kutatása és bevezetésének igénye terén. Ezt a tény támasztja alá a Közigazgatási Informatikai Bizottság (KIB) munkájának eredményeként létrehozott, a közigazgatási területen információbiztonsági ajánlásokat tartalmazó dokumentumgyűjtemény, amelynek első, hivatalos kiadása 2008-ban jelent meg.[204] A hazai információbiztonsági ajánlások dokumentumai az ISO/IEC 27000-es szabványcsalád útmutatásait hűen követik, figyelembe veszik a hazai szokásokat, az intézményrendszert, azok működését, fejlesztését és fenntartását a közigazgatási szférában. Nemcsak megjelenik a bizalmasság, a sértetlenség és a rendelkezésre állás hármas alapelv, de erre építi fel az információbiztonsági szabályozási rendszert. A közigazgatási területen, az információbiztonságon belül érinti a fizikai, logikai és személyi védelem, valamint biztonság kialakítására vonatkozó elengedhetetlen szabályozást. A dokumentumok már rögzítik az intézményi szabályozásra, de különös tekintettel a személyi és fizikai biztonságra, a hozzáférés menedzselésére, az adatvédelemre, az incidenskezelésre vonatkozó irányelveket és a vizsgálati, valamint az értékelései szempontokat. Az ajánlás az információs rendszer biztonsági vizsgálatához, biztonsági osztályba[205] és szintbe sorolásához olyan útmutatót nyújt, ami által

[204] A KIB 25. számú ajánlása: 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata, https://ugyintezes.magyarorszag.hu/dokumentumok/kib25ibiv.pdf, letöltés: 2022. július 19.

[205] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

bármely közigazgatási információs rendszer helyzetfelmérése és információbiztonsági értékelése megvalósítható.

2.4.7.3. INFORMÁCIÓBIZTONSÁGI SZABÁLYOZÁS

A szabványok, az Európai Uniós törekvések, ajánlások, rendeletek és törvények megjelenése előtt nemcsak nemzetközi színtéren, de hazánkban is törekedtek a tárolt információk szabályozására. Ennek megfelelően született néhány rendelkezés 1992-1996. között, amelyek kutatásom szempontjából is jelentős.[206] Az információbiztonság szabályozásához kapcsolódó rendelkezések érintik a személyes adatok, valamint az államtitkok és szolgálati titkok, továbbá az üzleti titok védelmét. A hivatkozott jogszabályok, ajánlások és a dokumentációk tartalma szerint vélelmezhető, hogy az információbiztonságot érintő hazai törvényi szabályozási törekvések és a későbbi szabályozási rendszer, melyet az Európai Unió és tagállamai tekintetében Magyarország elsők között alkotott meg és léptetett hatályba, összhangban van az uniós elvekkel és elvárásokkal, valamint a nemzetközi szabványi ajánlásokkal (ISO/IEC 27000-es szabványcsalád). A hivatkozott hazai jogszabályok vizsgálata megerősíti a H1 hipotézisben megfogalmazott felvetés igazolását.

2.5. AZ ADATVÉDELMI ÉS AZ INFORMÁCIÓBIZTONSÁGI FOGALMAK RENDSZEREZÉSE

Ebben a fejezetben bemutatásra került az információ fogalmával összefüggésbe került adatvédelmi és információbiztonsági szakkifejezések és jogintézmények. A fogalmak vizsgálata során megállapítottam, hogy jogszabályi szinten az Infotv. értelmében a személyes adatok és azok kezelésére, míg az IBtv. szerint különösen az információs rendszerrel

---

[206] 1992. évi LXIII., a személyes adatok védelméről és közérdekű adatok nyilvánosságra hozataláról szóló törvényt, amelyet hatályon kívül helyezett a 2011. évi CXII., az információs önrendelkezési jogról és az információszabadságról (Infotv.) törvénye.
1995. évi LXV., az államtitokról és a szolgálati titokról szóló törvény, amelyet hatályon kívül helyezett a 2009. évi CLV. törvény a minősített adat védelméről.
1995. évi CXXV., a Nemzetbiztonsági szolgálatokról, különösen az Információs Hivatal, Alkotmányvédelmi Hivatal működéséről szóló törvény.
1996. évi LVII., a tisztességtelen piaci magatartás és versenykorlátozás tilalmáról szóló törvény, amelyben megtalálható az üzleti titok védelme: „*Tilos a Polgári Törvénykönyvben meghatározott üzleti titkot tisztességtelen módon megszerezni vagy felhasználni, valamint jogosulatlanul mással közölni vagy nyilvánosságra hozni*."
1998. LXXXV. törvény A Nemzeti Biztonsági Felügyeletekről, amelyet hatályon kívül helyezett a 2009. évi CLV., a minősített adat védelméről szóló törvény.
2001. évi CVIII. törvény az elektronikus szolgáltatások (e-kereskedelem) szabályozására, amelynek érdekessége, hogy megtalálható benne az információ, mint fogalom a (2.§ e)-ban, amely szerint az „Információ: bármely, elektronikus úton feldolgozható, tárolható, továbbítható adat, jel, kép tekintet nélkül arra, hogy annak tartalma jogi védelemben részesül-e".
Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat .
2013. évi L. törvény, az állami és önkormányzati szervek elektronikus információbiztonságáról.

kontaktusba kerülő, leginkább biztonsági és védelmi szempontból megközelített meghatározásokat találtam. Megállapítottam továbbá, hogy az IBtv. által definiált fogalmi kör lényegesebb szélesebb spektrumú, mivel nemcsak információvédelmi és információbiztonsági szakkifejezéseket, hanem például szervezetekre vagy adatvédelemre vonatkozó megállapításokat is tartalmaz. Ennek hátránya az, hogy különösen a két jogszabály értelmező rendelkezései között redundancia és némi eltérés (adatkezelés) is tapasztalható. Véleményem szerint az adatvédelmi meghatározásokat elég lenne egy jogszabályban, leginkább az Infotv. rendelkezései között rögzíteni, és azokra hivatkozni, ezáltal elkerülhetővé válik az eltérés. Az IBtv. nem tér ki olyan fogalmak meghatározására, mint az adattovábbítás, ami meghatározó tényezője az információs rendszernek[207] vagy az információbiztonság, ami a címben is szerepel, és a információvédelem egyáltalán nem is fordul elő a jogszabály szövegében. A védelem több fajtája is meghatározásra került, így a „kibervédelem", az „adminisztratív védelem" vagy a „folytonos védelem", ugyanakkor tudjuk mi az a „a védelem" vagy a „a védelem érdeke", illetve mi a különbség a „védelem" és a „biztonság" között? Ezen meghatározások pontosítása a jogszabály tekintetében mindenképp szükséges. A „zárt védelem" meghatározása vonatkozásában az összes számításba vehető fenyegetések repertoárja akár napról-napra változik, ezáltal talán sose érhető el a „zárt védelem" szintje. Itt inkább az adott szervezetre vonatkoztatható fenyegetések csoportja lenne a megfelelőbb kifejezés, ennek következtében a fenyegetések csoportját is definiálni kellene, akár az értekezés 4.2.2.1 fejezete alapján. Az Infotv. tekintetében a magatartási kódex[208] magyar jellegzetességeinek és szükségességének hangsúlyozása hasznos volna az adatkezelők számára. E tekintetben a vonatkozó fogalmak (tisztességes és átlátható adatkezelés) jogszabályi szintű meghatározása vagy pontosítása szükséges. A fentiekben közölt, jogszabályokra vonatkozó vizsgálati eredményem szerint megállapítottam, hogy a jogszabályok értelmező rendelkezései ugyan követik az adatvédelmi és információbiztonsági szabályalkotási igényeket, mégis helyenként, némi pontosításra szorul. A jogszabályi szakkifejezések és meghatározásaik az egyetemi tananyagokban is megjelennek. A tananyagok és szakirodalom tekintetében ugyanakkor már sokkal színesebb meghatározásokkal találkozhatunk, akár az információbiztonsági tudatosság meghatározásának

[207]„számítógépek és elektronikus hírközlő hálózatok, valamint a működtetésük, használatuk, védelmük és karbantartásuk érdekében általuk tárolt, feldolgozott, visszakeresett vagy továbbított elektronikus adatok" összessége, Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.), az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról

[208] Európai Adatvédelmi Testület, 1/2019 iránymutatás az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről (2.0. változat) 2019. június 4.

vonatkozásában[209] [210] [211] [212] sincs egységes álláspont. A biztonságtudatosság, információbiztonsági tudatosság témakörhöz kapcsolódó szakkifejezések[213] [214] [215] pontosabb használatának érdekében az értekezésben az alábbi meghatározásokat és összefüggéseket használom.

Információbiztonsági tudatosság tekintetében megfogalmazom, hogy az információs rendszer adatkezelőinek, adatfeldolgozóinak, rendszerüzemeltetőinek, tulajdonosainak, vagy a rendszer által kezelt, illetve továbbított bármilyen információval kapcsolatba kerülő személyek azon képessége, hogy az információs rendszer biztonságának[216] fenntartásával összhangban megfelelő készséggel – úgymint érzékeléssel és megértéssel – rendelkezzen, valamint szándéka és képessége legyen további ismereteket szerezni ahhoz, hogy az információs rendszerekbe vetett bizalom erősítése érdekében, a rendszerrel kapcsolatos feladatokat, intézkedéseket, vagy bármilyen eljárásokat végrehajtsanak.

Információbiztonsági tudatosítás tekintetében megfogalmazom, hogy a információbiztonsági tudatosság fejlesztésére irányuló azon tájékoztatások, képzések, tréningek, oktatások és egyéb az érintett tudását gyarapító tevékenységek összessége, amely tevékenységek folyamán az érintett személy információbiztonsági tudatossági szintje növekvő tendenciát mutat. [217]

Információbiztonság tekintetében alkalmazom az ISO/IEC 27001 szabvány szerinti megfogalmazást, miszerint a CIA elvek teljesülése az információ vonatkozásában, továbbá

---

[209] Tarján Gábor, Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben, Budapest, 2020.
[210] Illéssy Miklós, Nemeslaki András, Som Zoltán, Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs Társadalom, Társadalomtudományi Folyóirat, 14 (1). pp. 52-73. ISSN 1587-8694, 2014.
[211] Nemeslaki András, Sasvári Péter, Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában, Infokommunikáció és jog, 2014/4.(60.), 169-177.o.
[212] Mádi-Nátor Anett, Kardos Zoltán, Nemzeti Közszolgálati Egyetem, Mádi-Nátor Anett, Kardos Zoltán, Információbiztonság-tudatosság gyakorlat, Nemzeti Közszolgálati Egyetem, https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsag-tudatossag-gyakorlat.original.pdf, letöltés: 2022. január 18.
[213] OECD Guidelines for the Security of Information Systems, 1992
[214] ISO Guide 73, Risk management, Vocabulary
[215] ISO 31000, Terms and definitions
[216] „A dolgoknak, életviszonyoknak olyan rendje, olyan állapot, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek nincs vagy alig van lehetősége, amelyben ilyentől nem kell félni.” Arcanum Digitális Tudománytár, Kézikönyvtár, A magyar nyelv értelmező szótára alapján
[217] „*Az információbiztonság-tudatosságnövelési program magában foglalja az adott szervezet általános felhasználóinak, kiemelt felhasználói jogokkal rendelkező vezetőinek, IT üzemeltetőinek, IT fejlesztőinek információbiztonsági tudatosítását*”
Mádi-Nátor Anett, Kardos Zoltán, Nemzeti Közszolgálati Egyetem, Mádi-Nátor Anett, Kardos Zoltán, Információbiztonság-tudatosság gyakorlat, Nemzeti Közszolgálati Egyetem, https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsag-tudatossag-gyakorlat.original.pdf, letöltés: 2022. január 18.

belefoglalható különösen a hitelesség, elszámoltathatóság, letagadhatatlanság és a megbízhatóság elve is.

Információvédelem tekintetében megfogalmazom, hogy logikai és fizikai védelem összessége, a védelem tekintetében pedig azon sérülékenységek és fenyegetések elleni intézkedések összessége, amelyek során megóvjuk információs rendszerünket a különböző információbiztonsági kockázati tényezőktől és az incidensek bekövetkezésétől, ezáltal teljesítve az információbiztonság alapelveit.

Információbiztonsági incidens tekintetében az ISO/IEC 27000 szabványcsalád alapján megfogalmazom, hogy olyan információbiztonsági események, amelyek veszélyeztetik az információbiztonságot.

Adatbiztonság a GDPR 5. cikke – A személyes adatok kezelésére vonatkozó elvek – szerinti adatvédelmi elvek teljesülése az adat vonatkozásában.

Adatvédelem a GDPR 25. cikkének alapján alkalmazott beépített és alapértelmezett adatvédelem, amely az adatkezelés során megfelelő technikai és szervezési intézkedéseket hajt végre, annak érdekében, hogy a GDPR 5. cikke – A személyes adatok kezelésére vonatkozó elvek – szerinti adatvédelmi elvek teljesüljenek, különösen az adattakarékosság, valamint a rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

Adatvédelmi jogsértés tekintetében megfogalmazom, hogy olyan személyes adatokat ért incidens, amely következtében sérül az adatvédelmi elv (GDPR 5. cikk).

Kiberbiztonság (Cybersecurity, Cyberspace security) az ISO/IEC 27000 szabványcsalád alapján, a CIA elvek megőrzése a kibertérben, továbbá belefoglalható különösen a hitelesség, elszámoltathatóság, letagadhatatlanság és a megbízhatóság elve is. Ugyanakkor a Cybersafety kifejezés alatt, az a feltétel értendő, amely ellen védett fizikai, szociális, pénzügyi, politikai, érzelmi, foglalkozási, pszichológiai, oktatási vagy más vonatkozású hiba, kár következményei, illetve hiba, baleset, sérülés vagy bármilyen más incidens a kibertérben[218], ami nem kívánatos a rendszer működése szempontjából. [219]

[218] „*A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.*"
Magyarország Nemzeti Kiberbiztonsági Stratégiája, 2012

[219] „*A kiberbiztonság és az információbiztonság közötti fogalmi különbség egyértelműen megfogalmazott a magyar jogszabályokban. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*

Kibervédelem tekintetében megfogalmazom, hogy logikai és fizikai védelem összessége a kibertérben. Védelem tekintetében pedig azon fenyegetések elleni intézkedések összessége, amelyek során megóvjuk információs rendszerünket a kibertérből érkező különböző támadásoktól, ezáltal teljesítve a kiberbiztonság alapelveit.

Kiberbűncselekmény vagy kiberbűnözés tekintetében megfogalmazom, hogy olyan bűnügyi tevékenység, amely során az információs rendszerben tárolt személyes adat vagy más információ, illetve az információs rendszer adott eszköze, szolgáltatása vagy alkalmazása a kibertérben elkövetett bűncselekmény közvetett vagy közvetlen célpontja, továbbá ebben a tekintetben a kibertér lehet forrás, eszköz, cél, illetve a bűncselekmény helyszíne is.

A fentiek tekintetében megállapítottam, hogy az adatvédelmi és információbiztonsági szakkifejezések egységesítése és konzekvens használata elengengedhetetlen mind a jogszabályok megalkotásának, mind pedig az oktatási tananyagok megalkotásának tekintetében.

2.6. RÉSZÖSSZEFOGLALÁS

Az évszázadok során megszokott szabályok fejlesztéséhez ismerni és érteni kell történetüket, az elmúlt korok szokásait, szabályait és az információs társadalom új igényeit is. Az információtörténet kutatásának eredményei az információbiztonság szabályainak megalkotásához, vagy igény szerinti megváltoztatásához elengedhetetlen. Az információ fogalma nagy utat tett meg az „*ideák*” világától az információelméletig, bár minden tudományágban jelen van, mégis legfőképp az információbiztonság, valamint az informatikai technológia bitorolja. Valószínű ennek oka, hogy az információelmélet leginkább a számítástechnika, az informatikai hálózat tanulmányozásához kapcsolható. Az információtörténet érdekessége, hogy az információ mai, informatikai vonatkozású fogalma igen fiatal, alig száz éves és a kapcsolódó információbiztonság jogintézménye is csak néhány évtizedes múltra tekinthet vissza. E tekintetben meglehetősen gyermekkorban lévő fogalommal

szerint az elektronikus információs rendszer biztonsága „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos”, míg a kiberbiztonság „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez”.”
Krasznay Csaba, Kiberbiztonsági K+F+I Európában, Fenntartható biztonság és társadalmi környezet tanulmányok V., Sorozatszerkesztő: Kis Norbert, Koltay András, Szerkesztette: Török Bernát, Budapest, 2020.

és intézményrendszerrel találkozhatunk, szemben a több ezeréves, ókori alapokat lefektető, filozófiai, állam-, matematikai és orvostudomány elméletekkel szemben. Vajon a legifjabb tudományág meghatározásai felveszik a versenyt az őskövületi tudományágakkal? Véleményem szerint, mindenképp. Az a tény, hogy fiatalabb és kiforratlanabb, nem jelenti azt, hogy alkalmazásával hátráltatná vagy megakadályozná a többi tudományág fejlődését, épp ellenkezőleg. Fiatalságával és dinamikus fejlődésével pozitívan hat a többiekre, és a kommunikáció felgyorsításával, a biztonságosabb csatornák és információs rendszerek használatával biztos közeget teremthet a többi tudományág számára. Az adatvédelmi és információbiztonsági jogintézmények, ezáltal a szabályozási rendszer párhuzamosan fejlődött az informatikai technológiával. A technikai megoldások műszaki és jogi szabályozási igénye és megvalósulása is jelentős. Úgy tűnik, hogy a két terület, úgymint az IT és a szabályozás egymásra jótékony hatással van egymásra, és kiegészítik egymást, egyik a másik nélkül nem „*élhet*", ugyanakkor megfigyelhető a két terület közti jelentős rivalizálás is, amely egyfajta versenyt, máskor kritikát eredményez.

Az első hipotézisem (H1) szerint feltételeztem, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és jogszabályi rendelkezések fejlődése a nemzetközi szabványügyi intézmények ajánlásaival és az európai szabályozással összhangban vannak.. A jelen fejezethez kapcsolódó kutatásom során megvizsgáltam a nemzetközi, elsődlegesen Európai Uniós, valamint példaként a németországi és a hazai adatvédelmi (GDPR, német szövetségi adatvédelmi törvény, Infotv.) és az információbiztonsági rendelkezések (IBtv.) és szabványi ajánlások (ISO/IEC 27001), jogtényezők történeti hátterét és fejlődését, jelentőségét, összefüggéseit, valamint az adatvédelmi alapelvek és szabályok alkalmazásának szükségességét, amelyet az adatvédelmi és információbiztonsági jogtörténet vizsgálatának, összehasonlító elemzésének jelen fejezetben található kivonatával prezentáltam. Az információ védelmére irányuló történeti áttekintés összefüggései rámutatnak arra, hogy az adatvédelemre, információbiztonságra vonatkozó alapelvek és rendelkezések megfogalmazása és alkalmazása indokolt a papír alapú és elektronikusan tárol személyes adatok védelmének kialakításában és fenntartásában egyaránt. A hazai adatvédelmi (Infotv.) és információbiztonsági (IBtv.) rendelkezések összhangban vannak a nemzetközi adatvédelmi rendelkezésekkel (GDPR, német szövetségi adatvédelmi törvény), valamint a nemzetközi információbiztonsági irányítási rendszer (ISO/IEC 27000 szabványcsalád, ISO/IEC 27001, A melléklet - ISMS) ajánlásával (az ISMS bemutatása a negyedik fejezetben található). Az adatvédelmi, információbiztonsági rendelkezések és szabványi ajánlások elősegítik a rendelkezések és szabványi ajánlások

alkalmazását, amelyet kutatásom során megjelentetett publikációk is igazolják.[220] [221] [222] A hivatkozott publikációkban szereplő statisztikai adatok rámutatnak arra, hogy a rendelkezések, szabványi ajánlások intézményi szintű, együttes alkalmazása kielégíti az információbiztonsági szabályozási igényeket is. Természetesen ez a megállapítás egy adott időszakban mért állapotot mutat. amely azt jelenti, hogy a rendelkezéseket nemcsak bevezetni és csak egy adott időszakban kell működtetni, hanem az így létrehozott információbiztonsági rendszer folyamatos fenntartása és fejlesztése (PDCA elvek alkalmazása) elengedhetetlen ahhoz, hogy a későbbiek során is teljesítse az információbiztonsági követelményeket[223].

A fejezetben részletezett adatvédelmi és információbiztonsági történeti áttekintés, a témával kapcsolatos vizsgált és hivatkozott jogszabályok, ajánlások és a dokumentációk tartalma alapján megállapítottam, hogy az adatvédelmi és információbiztonságot érintő hazai törvényi szabályozási törekvések és a megalkotott jogszabályok, melyeket az Európai Unió és tagállamai tekintetében Magyarország elsők között alkotott meg és léptetett hatályba, konszenzusban vannak az uniós elvekkel és előírásokkal (GDPR), valamint a nemzetközi szabványi ajánlásokkal (ISO/IEC 27000-es szabványcsalád). A hivatkozott hazai jogszabályok vizsgálata megerősíti a H1 hipotézisben megfogalmazott felvetésem igazolását, amely szerint a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és jogszabályi rendelkezések fejlődése a nemzetközi szabványügyi intézmények ajánlásaival és az európai szabályozással összhangban vannak.

Az adatvédelmi és információbiztonsági fogalmak vizsgálata során megállapítottam, hogy az egységes magyar az adatvédelmi és információbiztonsági szakkifejezések kiadása és rendszeres időszakonkénti felülvizsgálata, a technológiai fejlődéshez igazított fejlesztése szükséges. A felülvizsgálati eredmények alapján az Infotv. és IBtv. értelmező rendelkezéseinek kétévenkénti igazítása elengedhetetlen. Megállapítom továbbá, hogy a vonatkozó szakkifejezések korrelációjának vizsgálata és definiálása sem tisztázott, ugyanakkor ezen megállapítások az adatvédelem és az információbiztonság oktatás alapfogalmai.

---

[220] Ferenc, Leitold, Kálmán Hadarics , Eszter Oroszi , Krisztina Győrffy: Measuring the information security risk in an infrastructure, MALWARE 2015 10th International Conference on Malicious and Unwanted Software, Puerto Rico, 2015

[221] Győrffyné Holló Krisztina: Az információbiztonság jelentősége és története, GRADUS Vol 8, No 2 (2021), John von Neumann University, Hungary, Kecskemét

[222] Krisztina Győrffyné Holló, Adam Karisztl, Domino effect and other models in the IT process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

[223] Krasznay Csaba, Okoseszközök a kritikus információs infrastruktúrákban, Információ- és kiberbiztonság, Fenntartható biztonság és társadalmi környezet tanulmányok V., Sorozatszerkesztő: Kis Norbert, Koltay András, Szerkesztette: Török Bernát, Budapest, 2020. (kiberbiztonsági szempont)

3. AZ ADATVÉDELEM JELENTŐSÉGE, SZABÁLYOZÁS ÉS GYAKORLAT ÖSSZEFÜGGÉSEI

3.1. AZ ADATVÉDELEM JELENTŐSÉGE

A hazai internethasználat évenkénti felmérése rámutat arra, hogy az elmúlt 20 évben közel nyolcszorosára nőtt az internethasználók aránya, míg 2000. évben alig haladta meg a 10% -os értékét, addig 2020-ra több, mint 80% rendszeresen használta az internetet. A különböző X, Y, Z generációk internethasználata 90% feletti étéket mutat és hazánkban az internetet rendszeresen használók száma meghaladta a hatmillió főt. [224] A rendszeres internethasználat is indokolja a magasabb szintű és szigorúbb technikai, adatvédelmi és információbiztonsági szabályok alkalmazását. Gyermekeink már a digitális világban nőnek fel, ezért különösen indokolt, hogy az utcai közlekedés szabályainak megtanítása alapján, tanítsuk meg a digitális hálózaton való közlekedést és ezáltal a digitális társadalmi kultúrát, annak minden előnyével és veszélyével, valamint védekezési lehetőségével együtt. A gyermekek azok, akik védelmére kifejezetten oda kell figyelni. Az internetes kultúra hatással van a gyerekeink szokására, életvitelére és viselkedésére. Ma már a digitális oktatásnak köszönhetően napjuk egy részét az internet világában töltik, tehát az információs rendszereink megfelelő védelmi szintjének kialakítása és fenntartása fokozott figyelmet kíván. A megvalósult jogsértések és a konfliktuskezelési eljárások kezelése a gyermekkorú személyt illetően összetettebb és speciális feladat és javasolt a jogsértések és a későbbi konfliktusok kialakulásának megelőzése.[225] Kutatásom során az adatvédelmi és az információbiztonsági lehetőségek közül elsődlegesen a megelőzés típusú módszerek alkalmazását részesítem előnybe, amelyeket az adatvédelmi és információbiztonsági alapelvek és rendelkezések támogatnak, valamint a kutatásom során kapott eredmények[226] és a jelen fejezetben összegzett adatvédelmi statisztikai adatok is alátámasztanak. Eredménytelen megelőzési megoldások és bekövetkezett incidensek esetén alkalmazhatók az elhárítási, helyreállítási és szankcionálási lehetőségek. Mindezen eszközök alkalmazása költséges és speciális információbiztonsági intézkedéseket, adatvédelmi hatósági eljárásokat és esetlegesen adatvédelmi bírságokat eredményez. Ebben a fejezetben bemutatásra

[224] NRC Marketingkutató és Tanácsadó Kft., Nőtt az internetpenetráció, már 6 175 500 fő internetezik hazánkban, időszak: 2000-2019. https://nrc.hu/news/internetpenetracio-2/, letöltés: 2021. április 27.
[225] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Kulcs a Net világához! A NAIH tanulmánya a gyermekek biztonságos és jogtudatos internethasználatáról https://www.naih.hu/files/2013-projektfuzet-internet.pdf, 23-24.o., 2013., letöltés: 2021. április 27.
[226] Krisztina Győrffyné Holló, Adam Karisztl: Domino effect and other models in the it process, Gradus Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

kerülnek azok a nemzetközi és hazai statisztikai adatok, adatvédelmi incidensek és kevésbé kritikus, de figyelemfelhívó jellegű adatvédelmi tájékoztatási kötelezettségekkel foglalkozó ügyek, amelyek indokolttá teszik és igazolják az adatvédelmi szabályok megalkotását, a technológiai fejlődéshez igazított fejlesztését és mindenkori alkalmazását. Az adatvédelmi jogszabályok elsősorban a polgárok személyhez fűződő jogait védi és az adatvédelmi hatóságok működtetésével biztosítják az érintett adatvédelmi jogainak érvényesíthetőségét. A kutatásom során elsődlegesen a NAIH által közzétett adatvédelmi határozatokban közölt esetek és a határozatok vizsgálata alapján általam összeállított statisztikai kimutatáson (saját adatgyűjtésen alapuló táblázatok, grafikonok) keresztül szemléltetem az adatvédelmi alapelvek és szabályok (GDPR, Infotv.) betartásának szükségességét. Továbbá arra is szeretnék rávilágítani, hogy az adatvédelmi szabályok alkalmazása minden olyan esetben szükséges, ahol személyes adatot kezelnek vagy biztonsági mentés céljából tárolnak, illetve az adott információs rendszer segítségével továbbítanak, független attól, hogy az adatot papíron vagy elektronikus módon kezelik. A kutatásom során vizsgált nemzetközi és hazai adatvédelmi esetek statisztikai adatai rámutatnak az adatvédelmi szabályok és a hatásvizsgálat jelentőségére. A kutatásom során figyelembe vettem a GDPR életbe lépését, és a vizsgált időszakot ennek megfelelően állapítottam meg, legfőképp 2019-2021. közötti időintervallumot vettem figyelembe. A vizsgált időszakba a Covid-19 világjárvány is beletartozik, amikor fokozottabb volt a távmunka és következményei az adatvédelmi eljárásokban is megmutatkozott, legfőképp a tájékoztatási kötelezettség elmulasztásában vagy a hozzáférési jogsértésben. Véleményem szerint a következmények meghatározó oka elsődlegesen a „*humán error*” típusú felhasználói aktivitásban keresendő. A kutatásomhoz nemzetközi és hazai tudományos publikációk, hatóságok és adatvédelemmel foglalkozó nagyvállalatok által nyilvánosságra hozott, hiteles statisztikai adatait vizsgáltam, annak érdekében, hogy különösen az első (H1), második (H2) és harmadik (H3) hipotézisem adatvédelmi tényezőit igazolni vagy cáfolni tudjam. A fejezetben található kutatási eredmények kifejtéséhez és a háttérkutatáshoz dokumentum- és tartalomelemzési, kvalitatív, összehasonlító és statisztikai adatelemzéseket, továbbá empirikus kutatást, a matematikai logika alkalmazásával használtam.

3.1.1. ADATVÉDELMI JOGSÉRTÉSEK

Kutatásom során megállapítottam, hogy az adatvédelmi szabályok betartása és jelentősége kevésbé releváns az emberek számára egészen addig, amíg az incidens be nem következik,

amelynek során adataik veszélybe kerülnek, azzal visszaélnek, vagy anyagi kárt szenvednek.[227] Az incidensek elérik ma már az idősebb és a fiatalabb korosztályt egyaránt. Az egyik legkritikusabb kategóriába tartoznak azok az incidensek, amikor gyermekeink adataival, fényképeivel visszaélnek, azt illegális célra használják, nevükben üzeneteket küldenek, vagy zsarolnak. Az adatmegszerzés és a visszaélések egyre színesebb és színesebb megnyilvánulási formájával találkozunk nap, mint nap. A legnagyobb közösségi portálokat sem kímélik az adathalász hackerek, akik megkeserítve a felhasználók életét, rendszeresen a nevükben üzeneteket, reklámokat, játékra felhívást küldenek ismerőseiknek. 2021. évi adatvédelmi incidensek egyike a Facebook adatszivárgása volt. Az esettel kapcsolatban megállapították, hogy a cég online weboldalának adatbázisából több, mint 530 millió ember adata szivárgott ki, amelynek nagyrésze mobil telefonszám volt. A Facebook állásfoglalása szerint egy 2019. évi régi adatbázis adata került nyilvánosságra, és azóta az adatvédelmi jogsértést okozó biztonsági rést kijavították. Az úgynevezett régi adatvédelmi incidens következménye csak később okozott kárt, másfél évig a hackerek őrizték titkukat, majd egy blogon keresztül napvilágra hozták az adatokat. Az adatokat elemző kutatók szerint az adatbázis 106 ország 533 millió felhasználói profil adatát érintette. Ebbe beletartozott az Egyesült Királyság 11 millió Facebook felhasználója, továbbá 30 millió amerikai és 7 millió ausztrál felhasználót érintett.[228] A céggel szemben felmerült a szándékosság gyanúja is, hiszen a vezetőjének saját mobilszámát is megtalálták a letárolt adatbázisban. 2021. március végén a Facebook megállapította, hogy mintegy 600 millió felhasználó jelszavát, valószínű adatvédelmi és információbiztonsági szempontból nem megfelelő módon, tárolták, valamint 2018. szeptemberében az 50 millió felhasználóval kapcsolatos személyes adatok sérülhettek egy biztonsági hiba következtében. Sajnos, azt nem lehet tudni, hogy a nyilvánossá tett személyes adatok közül mennyi szivároghatott ki valójában. Időközben számos adatvédelmi vizsgálatot is indítottak a cég ellen,

[227] Krisztina Győrffyné Holló, Adam Karisztl: Domino effect and other models in the it process, Gradus Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.
[228] Possible Phishing Campaigns Arising from Facebook's Data Leak Government of Singapore, 2021.

mint például a hamburgi (német) felügyeleti hatóság[229], az Ír Adatvédelmi Bizottság[230] vagy a Fülöp-szigeteki Nemzeti Adatvédelmi Bizottság. Időközben a Spanyol Adatvédelmi Hatóság (AEPD) is folytatott hatósági adatvédelmi eljárást nagyobb cégekkel szemben. Az adatvédelmi hatósághoz 2018. április és 2019. szeptember között 191 panasz érkezett Vodafone adatvédelmi ügyekkel kapcsolatban, amelyben a kérelmezők jelezték, hogy kéretlen, többek között marketing célú telefonhívásokat és SMS-üzeneteket kaptak. A Vodafone céggel lefolytatott adatvédelmi hatósági eljárás keretében megállapították, hogy a cég megsértette többek között a GDPR 28. az adatfeldolgozóra vonatkozó, és 44. a személyes adatok harmadik országba vagy nemzetközi szervezetek részére történő továbbítása, az adattovábbításra vonatkozó általános elv cikkének előírásait,[231] továbbá a spanyol információs és telekommunikációs törvény rendelkezéseit. A hatóság több, mint 8 millió Euró adatvédelmi bírságot állapított meg az

---

[229] *„A DE-HH felügyeleti hatóság arra a következtetésre jut, hogy „A WhatsApp és a Facebook általi adatmegosztás az egyes vállalatok különböző céljait szolgálja. Amennyiben az ír adatvédelmi bizottság (IDPC) mint fő hatóság nem végez mélyrehatóbb ellenőrzést, felhívjuk a figyelmet az általános adatvédelmi rendelet 66. cikke szerinti sürgősségi eljárás lehetőségére.””, „…a WhatsApp IE harmadik felekkel és a többi Facebook-vállalattal is együttműködik marketingcélokból. Ugyanakkor nem áll rendelkezésre elegendő bizonyíték annak igazolására, hogy adatcsere történik, valamint, hogy az ilyen állítólagos adatkezeléssel összefüggésben a Facebook IE adatkezelőként vagy közös adatkezelőként jár el.” „A DE-HH felügyeleti hatóság által szolgáltatott információk, valamint a WhatsApp IE és a Facebook IE írásbeli beadványai alapján megállapítható, hogy a személyes adatok marketingkommunikáció és közvetlen üzletszerzés céljából történő kezelésével kapcsolatban a Facebook IE – legalábbis adatfeldolgozóként – a WhatsApp IE nevében kíván eljárni. Ugyanakkor az EDPB által elemzett információkból nem derül ki, hogy jelenleg adatcsere lenne folyamatban, illetve, hogy a Facebook IE saját marketingcélokra kezelné a WhatsApp felhasználóinak adatait.” „Az EDPB úgy véli, hogy a jelen eljárásban nem rendelkezik elegendő információval annak megállapításához, hogy sor került-e jogsértésre.” „Az EDPB felügyeleti hatóság ezért úgy véli, hogy ebben a konkrét esetben az általános adatvédelmi rendelet 61. cikkének (8) bekezdése nem alkalmazandó. Ennek megfelelően a DE-HH felügyeleti hatóság az általános adatvédelmi rendelet 66. cikkének (2) bekezdése szerinti megkeresésének sürgőssége nem vélelmezhető, és azt bizonyítani kell.” „az EDPB úgy határoz, hogy nem szükséges végleges intézkedéseket elfogadni a Facebook IE-vel szemben*.”
A hamburgi (német) felügyeleti hatóság az általános adatvédelmi rendelet 66. cikkének (2) bekezdése szerinti, a Facebook Ireland Limitedre vonatkozó végleges intézkedések elfogadásának elrendelésére irányuló kérelméről szóló 01/2021. sz., sürgősségi eljárás keretében elfogadott kötelező erejű határozat, Európai Adatvédelmi Testület, kötelező erejű határozata, Elfogadás időpontja: 2021. július 12., https://edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_hu, letöltés: 2022. július 21.

[230] C-311/18. sz. ügy, Data Protection Commissioner kontra Facebook Ireland Limited, Maximillian Schrems

[231] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)
28. cikk Az adatfeldolgozó, (1) „*Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.*”
V. FEJEZET,44. cikk Az adattovábbításra vonatkozó általános elv, „*Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, e rendelet egyéb rendelkezéseinek betartása mellett, ha az adatkezelő és az adatfeldolgozó teljesíti az e fejezetben rögzített feltételeket. E fejezet valamennyi rendelkezését alkalmazni kell annak biztosítása érdekében, hogy a természetes személyek számára e rendeletben garantált védelem szintje ne sérüljön*.”

adatvédelmi rendelkezések rendszeres és súlyos megsértése miatt.[232] A spanyol hatóságon kívül más európai adatvédelmi hatóság is foglalkozott adatvédelmi incidenssel, és állapított meg bírságot, így a Holland Adatvédelmi Hatóság (DPA) 475 000 Euró adatvédelmi bírságot szabott ki az utazást és szállást közvetítő vállalat nem tartotta be az adatvédelmi incidensbejelentés, hatósági határidőre vonatkozó előírásokat. Az adatvédelmi jogsértés következtében, a bűnözők több, mint 4000 ügyfél személyes adatait szerezték meg, többek között közel 300 ember hitelkártya adatát.[233] A statisztikai adatok megmutatják, hogy a hatóságok adatvédelmi hatósági eljárás indítására vonatkozó feladata évről évre nő, mivel az adatvédelmi ügyek és incidensek száma is jelentősen növekszik. Az incidensek számossága, az érintettek személyes adatainak sérülése vagy elvesztése, valamint az olyan adatvédelmi ügyek, mint például az érintetti adatvédelmi jogok gyakorlásának megakadályozása rámutat arra, hogy a nemzetközi egyezmények elfogadása, az adatvédelmi szabályok megalkotása, nemzetközi rendeletbe és nemzeti törvénybe iktatása, valamint az adatvédelmi hatóságok adatvédelmi jogkörrel és hatáskörrel felruházása, segítséget nyújthatnak az érintettet ért, adatvédelemi jogsértésekkel kapcsolatos esetek tisztázásában, amennyiben az adatvédelmi jogok helyreállítása, az adatvédelmi incidens kezelése csak jogi eszközökkel oldható meg. Az adatvédelmi ügyek között találunk kritikus és kevésbé kritikus eseteket is. A NAIH által közzétett nyilvános határozatok statisztikai adatait figyelembe véve, a kevésbé kritikus esetek, különösen az adatvédelmi tájékoztatási kötelezettséggel, az érintett hozzáférési, törlési jogának gyakorlásával összefüggő ügyek tekintetében csak részében volt szükség adatvédelmi bírság megállapítására. A 2020. évi statisztikai adatok alapján 15 hozzáférési jogot érintő ügyben 6 alkalommal, míg 23 tájékoztatási kötelezettséget érintő ügyben 12 alkalommal állapítottak meg adatvédelmi bírságot. Az adatvédelmi incidensek ügyében lefolytatott adatvédelmi hatósági eljárásokban szinte minden esetben adatvédelmi bírságot is megállapítottak. Ezek közül kiemelendők azok az ügyek, amelyekben az adatkezelő nem megfelelő módon, az adatvédelmi és információbiztonsági követelmények figyelmen kívül hagyásával kezelte, vagy tárolta a személyes adatokat, és azok nyilvánosságra kerültek, és ezáltal adatvédelmi jogsértést követett el.

[232] Spanish DPA Fines Vodafone Spain more than 8 Million Euros, https://edpb.europa.eu/news/national-news/2021/spanish-dpa-fines-vodafone-spain-more-8-million-euros_hu, letöltés: 2021. április 24.
[233] Brian Daigle, Mahnaz Khan, The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities, Journal of International Commerce and Economics, 2020.

3.1.2. ADATVÉDELMI STATISZTIKAI ADATOK

Az uniós és a nemzeti adatvédelmi szabályok értelmében garantálni kell az adatgyűjtés tárgyát képező személyes adatok védelmét. Az adatvédelem jogtörténeti kutatásom eredménye rámutatott arra, hogy a személyes adatok számítógépes adatrögzítésével megnövekedett a személyes adatokra vonatkozó védelem jelentősége, mind a szabályozás, mind a gyakorlati megvalósítás terén. Az Európa Tanács 1981. január 28-i 108. számú, *az egyéneknek a személyes adataik gépi feldolgozása során való védelméről* szóló egyezmény rámutat a személyes adatok és a magánélet tiszteletben tartásának fontosságára. Személyes adataink illetéktelen kézbe kerülése és azzal való visszaélés nagymértékű károkat tud okozni az érintett életében, veszélyezteti magán- és családi életét, így tanulmányait, munkahelyi pozícióját és életpályáját, hatással van a pénzügyi tevékenységére és befolyásolja családjának, legfőképp az incidensben ártatlan, de a következményeket elszenvedő gyerekeinek mindennapjait. Egy hanyagság vagy szándékosság okozta incidens felbecsülhetetlen következményekkel járhat, ami megsemmisítheti egy felépített élet munkáját. A személyes adatokat nemcsak a számítógép feltalálása óta gyűjtjük és tároljuk, de kezdetben leginkább tudományi, ipari, kereskedelmi, valamint hivatali célzattal, papír alapú, majd elektronikus nyilvántartások létrehozásának, valamint mindennapi tevékenységünk és az ügyvitel, visszakereshetőség megkönnyítésének okán. Ebből az okból származóan lehetőség volt családfakutatásra, népességnyilvántartásra, iparoslevél vagy diploma kiadására, I. illetve II. Világháborúban eltűntek felkutatására. A digitalizálás jelentősége, hogy több évszázadra vagy akár évezredre visszanyúló nyilvántartások és dokumentumok immár nemcsak a múzeumokban, könyvtárakban vagy a levéltárakban érhetőek el, ma már elektronikus módon kereshető adatbázisban tárolhatók, és a belőlük összeállított adathalmazból, statisztikai következtetéseken túl akár egy adott egyén családi háttere is felkutatható. Az adatgyűjtés és -tárolás módszere az elmúlt évtizedek során az információs rendszerek, valamint az Internet megjelenésével folyamatosan változott. Az információs technológiai fejlődés következtében lehetőségünk van arra, hogy vásárlásainkat, jelentkezésünket egy állásra illetve egészségügyi vizsgálatra, vagy akár banki hiteligénylésünket online módon intézhessük, mindezt személyes adataink megadásával, valamint a célhoz kötött, nyilvántartáshoz kapcsolódó adattárolásra és adatellenőrzésre vonatkozó hozzájárulással. Az információs rendszerek interoperabilitási képességének kihasználásával a személyes adatokat tartalmazó adatbázisok tartalma összefésülhetővé vált, és talán emberi felfogással már fel sem mérhető méretűvé duzzadt. A mai technológia segítségével élethű, digitális profil, avatar létrehozható, amely ismeri a múltat, rögzíti a jelent és

prognosztizálja a jövőt. A mesterséges intelligencia segítségével megállapítható az emberi reakció[234] és az esetleges egészségügyi állapot is. Tehát, ha azon elmélkedünk, mennyire van jelentősége az adatvédelemnek, az adatvédelmi szabályok megalkotásának és gyakorlati alkalmazásának a válasz a mesterséges intelligencia korlátlan alkalmazásában rejlik, aminek útját a szabályozott és a szabályokat megkerülő tevékenység befolyásolja. A kérdés pedig az, megéri-e az utóbbi úton elindulni, vállaljuk-e annak következményét, hogy a pillanatnyi lehetőségnek örvendve nem számolunk az adatvédelmi incidensek okozta károkkal. A jelen Uniós és hazai előírások szerint az adatvédelmi szabályokat mindazoknak a vállalkozásoknak és köz- vagy magánjogi szervezeteknek be kell tartaniuk, amelyek termékeiket – legyen az fizikai valósággal bíró árucikk, vagy szolgáltatás – értékesik az Unió területén. Az uniós adatvédelmi szabályok vonatkoznak az Unió területén forgalmazott vagy szolgáltatást nyújtó termékekre, amelyek képesek a személyes adatkérésre, -feldolgozásra és -továbbításra független attól, hogy azok felhasználása, az üzemeltető székhelye, vagy telephelye az Unió területén belülre vagy kívülre esik. Tehát a szabályok vonatkoztathatók az Unióban használható közösségi weboldalakra, az online kereskedelmi honlapokra és azokat üzemeltető vállalatokra, szervezetekre egyaránt. Adatvédelmi szempontból nem számít, milyen az adat megjelenési formája, úgymint digitális vagy papíralapú adatokról van-e szó. Ha olyan információk kerülnek tárolására vagy feldolgozására, amelyek alapján az érintett személyt közvetlenül vagy közvetett módon azonosítani lehet, a hatályban lévő adatvédelmi előírásokat mindenképpen alkalmazni kell. A GDPR és az Infotv. adatvédelmi szabályozásnak köszönhetően a digitális világ szabályozott keretek között folytathatja útját, így például a weboldalt használó látogatót tájékoztatják adataik tárolásáról és a nyomkövetés módszeréről. Ez a módszer a GDPR előírások hatályba lépése előtt is létezett, azzal a különbséggel, hogy a weboldalt látogató nem tudott róla. A látogatói adatok (sütik) legalább olyan célt szolgálnak, mintha az érintett személy bokájára fizikai nyomkövetőt csatolnának, és mozgását közzé tennék egy figyelő csoport által megtekinthető digitális térképen. Digitális világunkban számos publikus és kevésbé ismert lehetőség rejlik, a kérdés csupán az, mire és hogyan használjuk. Önmagában az a tény, hogy sikerült részben szabályozni a sütik világát, és felhívni a figyelmet a profilozás előnyeire és hátrányaira, mindezt szabályozott kereteken belül, rendkívül nagy teljesítmény, mivel az európai statisztikák szerint az európai lakosság nagy része, és a felmérés szerinti 56%

[234] Megjegyzés: Philip K. Dick novellái és Steven Spielberg, Különvélemény populista, szórakoztatóipar által előállított termékek jórészt kitaláción alapulnak, ugyanakkor a bennük rejlő néhány megoldás napjaink vagy jövőnk részese. A gondolatok teremtik a jövő technikáját, akár az MI esetében.

érvényesíti az adatvédelmi beállításokra vonatkozó jogokat.[235] Ugyanakkor szubjektív tapasztalatom szerint, nem mehetünk el azon reakciók mellett, amelyek a „*Birodalom visszavág*" megnyilvánulására utalnak, úgymint „*hogyan tegyük bosszantóvá a sütik beállítását*". Véleményem szerint a sütik egyre bonyolultabb beállítása az átlagos felhasználót idegesíti, ezért hamar ráun a beállítások ismétlésére, míg végül, a békesség kedvéért inkább engedélyezi az összes sütit. A különbség pedig a korábbi adatkezeléssel ellentétben, most önkét engedélyezte az adatainak felhasználását, egyben a profilozás kialakíthatóságát. Az egyre részletesebb információbiztonsági és adatvédelmi szabályozás, valamint a fejlett informatikai technológia támogatja mindennapi életünket, ugyanakkor a napjaink részévé vált a Világ különböző részeiről érkező támadási kísérletek és az incidensek megakadályozása, vagy az általuk okozott kár helyreállítása. Immár egyre több intézmény igényli az automatikus, illetve a mesterséges intelligencia által nyújtott megoldások alkalmazását a védelmi technológiában is. A helyi tűzfal szabályokat, a szerver és a végponti védelmet úgy konfigurálják, illetve alakítják ki, hogy az akár alkalmas legyen a beállított védelem továbbfejlesztésére, taníthatóságára. A támadási minták megjegyzésével, az információvédelmi mechanizmusok egy része tanítható, fejleszthető és az adatvédelmi és információbiztonsági alapelvek és a szabályok figyelembe vételével folyamatosan finomítható. Mindez sokszor kevésnek tűnik, hiszen a technológiai fejlődéssel, ami a hardveres és szoftveres megoldásokban egyaránt megmutatkozik, a technikai konfigurációkat tovább kell fejleszteni, finomítani és még így is megtörténhet *néhány* nem várt incidens. Az állandósult adatvédelmi és információbiztonsági alapelvek mentén kialakított és továbbfejlesztett technológiai megoldások sokat segítenek a preventív intézkedések megvalósításában és általánosan elfogadott álláspont, hogy az alapelvek mentén megvalósult preventív gyakorlati intézkedések hatékonysága jónak mondható. Természetesen teljes mértékű biztonság, illetve védelmi intézkedés nem létezik, mivel mindig van gyenge pont, ami adott esetben kihasználható. Amennyiben a gyenge pontot a támadók megtalálják, úgy az adatvédelmi vagy információbiztonsági incidens megvalósul. A COVID-19 vírus által okozott világjárvány idején megnövekedett az információs eszközök használata, legfőképp a tanulás és az otthoni munkavégzés okán, ezzel párhuzamosan a lehetőségeket kihasználva megnőtt a rosszindulatú adatbányász és a hacker műveletek száma és károkozásának mértéke. Évente több nagyvállalat végez statisztikai kutatásokat, az incidensek

[235] Uniós adatvédelmi szabályok, dokumentumtár, Vegye át az irányítást GDPR virtuális személyazonossága fölött!, 2019., https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_hu#az-ltalnos-adatvdelmi-rendelet-pozitv-eredmnyek, letöltés: 2021. április 21.

mértékével, az adatlopások feltérképezésével kapcsolatban. A Sans Institute[236] évről-évre támogatja az adatvédelmi és információbiztonsági riportok elkészítését és publikálja a statisztikai felmérések eredményét. Az ENISA által támogatott és hivatkozott hiteles felmérések is mutatják, hogy a statisztikai adatok rendkívül nagy adathalmazból kerültek ki és a világ minden tájáról származó események és jogsértések ezreinek statisztikai eredményén alapul, továbbá 16 különböző iparág és négy világrégió adatait tartalmazza. A 2020-ban összefoglalt riport hátterében összesen 157.525 eseményt elemeztek és ebből több, mint 32.000 eseményt és 3.900 jogsértést analizáltak, amelyek megfeleltek a minőségi előírásoknak. Az összegyűjtött 157.525 esemény közül 108.069 esetben hitelesítő adat megszerzése volt a cél, amelyek közül kiemelkedett a bankszámlát érintő jogsértés vagy a felhőszolgáltatások tevékenységét célzó incidens. [237] [238] Az éves, nagy szakértelmet igénylő kutatói munka alapú jelentéseket tudományos elemzésekhez is felhasználják. A jelentés olyan összegyűjtött információkból áll, amelyek alapja események, jogsértések és jogsértés minták, és amelyek részletes információkat nyújtanak a tényeken alapuló döntések meghozatalában, a kockázatok feltárásában és a szükséges intézkedések megvalósításában. A statisztikai elemzés hátterében tehát nagymértékű adatgyűjtés áll. A „*data breach*” egy olyan incidens típus, amely esetben az információk vagy információs rendszer egy része engedélyezett jogosultság nélkül elérhetővé válik és az illetéktelen hozzáférők a lehetőséget kihasználva legfőképp személyes adatokat szereznek meg, általában rosszindulatú szándékkal, ami potenciális veszteséghez vezethet, vagy hozzájárulhat további információszerzéshez, illetve azokkal való visszaéléshez. Az úgynevezett „*emberi hibák*” jelentősen befolyásolják az adatvesztés és a károkozás mértékét. Emberi mulasztás lehet, különösen bizonyos szolgáltatások konfigurálása és telepítése során is, amikor rendszerek és az adatok, általában nem szándékos jellegű publikussá tételét vagy továbbítását eredményezhetik. A matematikai szűrések és statisztikai elemzések eredménye a statisztikai kimutatás, amely a 3.950 jogsértés ágazat részletezett adatait mutatja meg. Az ágazatok közül kiemelendő az egészségügy (521 jogsértés), a pénzügyi ágazat (448), a közigazgatás (346), az információs technológia (360) vagy a felsőoktatás (228). A statisztikai adatok rámutatnak a kiemelten védendő területekre és a megelőző technikai tevékenységek

[236] Sans Institute, Data Breach Report, (DBR) 2020., https://www.sans.org/blog/2020-data-breach-incident-report-dbir/, letöltés: 2021. március 30.
[237] Verizon Data Breach Incident Report 2020.
[238] „Verizon Data Breach Incident Report” (DBIR) 2020, Wagner, Paul, Third Party Breaches - A Survey of Threats and Recommendations, United States, 2021. SSRN http://dx.doi.org/10.2139/ssrn.3782822, letöltés: 2022. február 26.

fokozottabb igénybevételére is.[239] [240] A védelmi szintet az adatvédelmi és az információbiztonsági alapelvek figyelembe vételével lehet magasabb szintre emelni a meglévő technikai, úgymint biztonságtechnikai és informatikai, valamint matematikai megoldások együttes használatának segítségével.[241] A hivatkozott tanulmányokban alkalmazott adatelemzési módszer szerint az adatokat hiteles forrásokból állítják össze, és táblázatos formában jelenítik meg, az adatelemzési vizsgálathoz százalékos- és átlagszámítás módszereket alkalmaznak a különböző típusú minták előállításához. A minták segítségével analizálták a különböző forrásból származó adatokat és következményeket, célzottan az adatszivárgás, valamint különböző típusú támadások viselkedésének elemzésére, végezetül idősoros elemzést alkalmaznak az adatsérülések, adatvesztések előre jelzésére.[242] Kutatásom során a bemutatott adatelemzési módszert alkalmaztam a kockázatkezelés[243] adatelemzési és összehasonlító vizsgálata során. Az elemzés során megnevezett „*fenyegetés szereplői*" a „*threat actor*", valamint a „*threat action*". A „*threat actor*", maga az elkövető, aki az adathalász tevékenységet elindítja, vagy aki a személyes adatokat tartalmazó dokumentumokat eltulajdonítja. A „*threat action*", a fenyegetés, illetve a rosszindulatú cselekedet, amelyek hét fajtája lehet, így különösen a „Malware" az események 17%-a, a „Hacking" az események 40%-a, a „Social", az események 22%-a, a „Misuse" az események 8%-a, a „Physical", az események 4%-a, az „Error", az események 22%-a, valamint az „Environmental". A felmérés által közölt események lehetnek adatvédelmi jogsértések és biztonsági incidensek. Az előbbiekben felsorolt eseményeket, a magas szintű technológiai műveletekkel, tehát szerver feltöréssel, rosszindulatú programok telepítésével, emberi viselkedést kihasználó adathalászattal és egyéb rendkívül nagy károkat okozó tevékenységekkel lehet elérni. A „Variety", amely az előző két kategória variációi, mint például olyan hacker vagy bűnözői csoport, az „SQL injection" vagy a „brute force" típusú műveletekre specializálódott.

Az ENISA és a Verizon által vizsgált incidensek adatainak vizsgálata szerint összegeztem az adatvédelmi jogsértésekhez kapcsolódó statisztikai adatokat, amely szerint az elszenvedő „*áldozatok*" 72%-a nagyvállalat, 58%-a természetes személy, akinek személyes adatai sérültek,

[239] ENISA Data Breach, Threat Landscape 2020
[240] ENISA Threat Landscape 2021
[241] Kálmán Hadarics, Krisztina Győrffy, Bálint Nagy, László Bognár, Anthony Arrott, Ferenc Leitold: Mathematical Model of Distributed Vulnerability Assessment, In: Jaroslav, Dočkal; Milan, Jirsa; Josef, Kaderka (szerk.) Proceedings of Conference SPI 2017: Security and Protection of Information, Brno, Csehország: University of Defence, (2017) pp. 45-57. 13 p.
[242] M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, R. A. Khan, Healthcare Data Breaches: Insights and Implications, Healthcare 2020, 8(2), 133; https://doi.org/10.3390/healthcare8020133
[243] Krisztina Győrffyné Holló, Adam Karisztl, Domino effect and other models in the IT process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

valamint 28%-a kisvállalkozó volt. A jogsértések 86%-a pénzügyi indíttatású, 37%-ában tulajdonítottak el vagy használtak hitelesítést szolgáló adatokat, és 22% adathalászat volt. Az adatok alapján megállapítottam, hogy a bejelentett, de nem megerősített incidensek vonatkozásába a DoS támadás és az adathalászat, míg a jogsértések kategóriájában az adathalászat és az ellopott hitelesítő adat állt az élen. Az adathalászat 96%-ában email típusú, míg 3%-ában weboldalon keresztül érkező aktivitás a jellemző és általában a hitelesítésre szolgáló adatokat próbálnak megszerezni. Véleményem szerint az adathalászat a támadók számára egy kényelmes és eredményes módszer, amely során arra építenek, hogy kihasználják az emberi jóhiszeműséget. Az adathalász tevékenység és az igazolt incidensek száma még mindig emelkedő tendenciát mutat, tehát az eredményességének kulcsa a gyenge láncszem, a hiszékenység. A felmérés alapján érdemesnek tartom az oktatás, az egészségügyi szolgáltatás és közigazgatás értékeléseit kiemelni, amely releváns lehet jelen értekezésben adatvédelmi, információbiztonsági helyzetfelmérés, rendelkezések jelentőségének és módszerek bemutatása szempontjából. A statisztikai adatokat vizsgálva megállapítható, hogy az oktatás ágazatban az adathalász adatvédelmi jogsértések száma magas, közel az esetek harmada (28%), valamint hitelesítő adat alapú hacker támadás és adatvédelmi jogsértés 23%-ban fordult elő. 2020-ban az incidensek 80%-ában Ransomware okozta az adatsértést, míg egy évvel korábban 48%-ban, tehát a növekedés drasztikus mértékű. A jelentés rámutat arra, hogy a Hatóságok felé indítandó adathalász tevékenységet tapasztaló bejelentési kötelezettség terén hiányosságokat és mulasztásokat tapasztaltak. Saját tapasztalataim alapján a bejelentés azért lenne fontos, mert ezáltal a központi figyelmeztető rendszerbe is bekerül az esemény, így további intézményeket fel tudnak készíteni a támadási kísérletre és az incidens, valamint az adatvédelmi jogsértés elkerülésére. Véleményem szerint, ha egy intézmény elmulasztja a bejelentési kötelezettséget, vagy később teszi meg, úgy a korai eseményfigyelmeztető rendszer sem éri el megfelelő hatását, így a támadási kísérlet nagyobb eséllyel veszélyezteti a többi intézmény információs rendszerét és a hacker nagyobb valószínűséggel fog sikeres támadást és adatlopást végrehajtani. Az elemzés szerint ebben az ágazatban a weboldalon és az email-en keresztül terjedő rosszindulatú programok által okozott események száma jelentősebb, mint más ágazatban. Tekintettel az ágazat jellegére, véleményem szerint egyértelmű, hogy az incidensek jelentős mértéke a hallgatói adatokhoz kapcsolódik. A hallgatók a személyes adataikat tartalmazó email fiókokat, saját informatikai eszközeiket olyan legfőképp nyilvános hálózaton használják, amelyek kevésbé védettek és nyilván adataik nagyobb veszélynek vannak kitéve, mint egy privát hálózatban. Az oktatási ágazatban általában vitára ad okot az, hogy az oktatói hálózaton

milyen szintű védettséget, mely részére terjesszék ki. Ezért sok esetben elszeparálják a védett oktatói, hallgatói és intézményi gazdasági információs rendszereket, a hálózati eszközöket és szegmenseket, valamint a hallgatói szférát kiszolgáló hálózati és információs rendszereket egymástól (itt példaként említhető a veszprémi általános- és középiskolák, ahol személyesen is közreműködtem a hálózatok kiépítésénél, a SULINET program keretében). Az információs rendszereket bár elszeparált módon kell kialakítani, de a közöttük az adatáramlást nem szabad az indokolt mértékű szigorú szabályok alkalmazásán felül akadályozni. A hallgatóknak és az oktatóknak olyan hálózati szférából is el kell tudni érni adataikat, adatkezelés és adatfeldolgozás céljából, amely kevésbé védett, mint az adott intézmény területén, így a kollégiumi, a könyvtári büfé hálózatából is biztosítani kell az adatok biztonságos adatáramlását. A COVID-19 vírus által okozott világjárvány idején a távoktatás és a távmunka is egyre jobban előtérbe kerül, így immár az otthoni hálózati környezetet is a munkavégzés vagy az oktatás, tanulás részévé vált. Vannak olyan technikai megoldások, amelyek a hálózaton áramló adatok védelmét szolgálják, mint például a virtuális magánhálózat (VPN), zárt hálózatban folytatott távoktatás (Moodle, Kréta, Skype, Google Classroom, Microsoft Teams vagy egyéb saját fejlesztésű e-learning rendszer), ugyanakkor az értekezésnek nem témája ezen eszközök biztonsági vagy technológiai ismertetése, a rendszerek palettáját csupán lehetősségként említettem meg. Amennyiben a zárt hálózati eszközöket megfelelően alkalmazzák a hallgatói, oktatói és munkavállalói szférában nemcsak az adatkommunikáció terén is nagyobb biztonsági szint érhető el, de egyéb, a távmunka olyan követelményei, mint a jelenlét, vagy az egységes technikai megoldások használata is könnyebben teljesíthető. Ugyanakkor sem az adatvédelmi jogszabályi rendelkezés vagy információbiztonsági ajánlás, sem a fizikai vagy a logikai szeparálás, a tűzfal és a szegmens konfigurálás nem ad kellő védelmet a nyílt hálózatból kiszivárgott vagy megszerzett, hallgatói, oktatói vagy akár rendszergazdai adatokból származó hitelesítési adatokat, a védett oktatási rendszerben felhasználó hacker műveletek ellen. A statisztikai adatok ebben az esetben is rámutatnak arra, hogy az adatvédelmi alapelveket és a technikai megoldásokat ki kell egészíteni a felhasználói tudatos tevékenységek megerősítésével.

Az oktatási ágazat tekintetében vizsgált események szerint[244] [245] a 819 incidensből, 228 esetben volt legfőképp személyes adatokat érintő adatközzététel, az elkövetés irányát tekintve 67%-ban

[244] Verizon Data Breach Incident Report 2020.
[245] „Verizon Data Breach Incident Report" (DBIR) 2020, Wagner, Paul, Third Party Breaches - A Survey of Threats and Recommendations, United States, 2021. SSRN http://dx.doi.org/10.2139/ssrn.3782822, letöltés: 2022. február 26.

volt külső és 33%-ban belső indíttatású, az incidensek 92%-a pénzügyi haszonszerzés célzatú volt, az adatsértés tekintetében személyes adatot ért 75%-ban, okmányt és hivatalos iratot érintett 30%-ban. Az incidensek következtében meghozott intézkedések típusai, különösen a biztonságtudatosság képzési program, a határvédelem, a biztonsági konfiguráció kialakítása és végrehajtása, amely összhang van saját kutatásom kockázatkezelése során megfogalmazott intézkedési típusokkal, így legfőképp a biztonságtudatosság képzési programmal és a biztonsági konfiguráció kialakítása és végrehajtása típusú intézkedéssel. A következő, a vizsgálatom során említést érdemlő ágazat az egészségügy. A vizsgált adatok szerint a támadói csoportok legfőképp a zsarolóvírus típusú támadási eszközökkel célozták meg az incidensben érintett intézményeket. Legfőképp az alapvető emberi tévedést, hiszékenységet használták ki, ezen kívül, ugyanakkor a belső visszaélések száma csökkent. Az egészségügyi ágazatban vizsgált események szerint a 798 incidensből, 521 esetben volt legfőképp személyes adatokat érintő, megerősített jogsértés alapú adatközzététel (adatszivárgás), ami egy évvel korábban 304 volt. Az elkövetés irányát tekintve 51%-ban volt külső és 48%-ban belső indíttatású, egy évvel korábban külső 42%, míg a belső 59% volt, az incidensek 88%-ának célja a pénzügyi haszonszerzés volt, az adatsértés tekintetében személyes adatot ért 77%-ban, orvosi iratot érintett 67%-ban, egyéb okmányt, dokumentumot pedig 18%-ban. Az elemzésemmel összefüggő vizsgálatom eredménye rámutat arra, hogy az egészségügyi intézményekben egyre gyakoribb, hogy a weboldalakat összekötik a belső adatbázissal, így az adatokat könnyedén át tudják szinkronizáltatni az intézményi adatbázissal, aminek a lényege, hogy a beteg az időpontkéréstől, a kezelési státuszon át a diagnózis eredményéig, minden számára lényeges információhoz hozzájuthat. Természetesen a webportálok mögötti adathalmaz nemcsak a betegek számára nyújthat kielégítő információt, de az illegális hozzáférők is kellőléppen érdeklődnek a különleges adatok iránt, amely immár jövedelmező célponttá vált. Tekintettel az egészségügyi ágazatban használt különleges adatokra 41 eseményt kiemelten kezeltek és az incidensek következtében meghozott adatvédelmi intézkedéseket az oktatási ágazatban használtakkal is kiegészítették. További vizsgálat alá vettem a közigazgatásból származó adatokat, amelyek kellőképp felkelthetik a támadók figyelmet, hiszen nemcsak a zsarolóvírussal próbálják megbénítani az adott állam közigazgatásának működését, de ezen a területen jelentősek a konfigurációs hibák és a nem megfelelően felügyelt adatátvitel sérülékenységét kihasználó legkisebb mértékű adatvesztések, adatsérülések vagy adatlopások, illetve következményként az adatszivárgás is. A kormányzati és a közigazgatási bizalmas adatok hanyagságból vagy szándékosságból eredő veszélyeztetése, jelentős károkat tud okozni

a nyilvánosságra kerülés által. Ez okból ebben az ágazatban a lehető legkisebb tévedés sem engedhető meg, és az adatvédelmi kockázat a lehető legkisebb mértékűek lehet. A közigazgatásban vizsgált események szerint 6843 incidensből, 346 esetben volt legfőképp személyes adatokat érintő, megerősített jogsértés adatközzététel, az elkövetés irányát tekintve 59%-ban volt külső és 43%-ban belső indíttatású, az incidensek 75%-a pénzügyi haszonszerzés és 19%-a kémkedés célzatú volt, az adatsértés tekintetében személyes adatot ért 51%-ban, okmányt, dokumentumot pedig 33%-ban. Megállapítottam, hogy a végrehajtott és nyilvánosságra hozott intézkedések hasonlóak voltak, mint az oktatási ágazatban. A közigazgatásból, tekintettel a különleges és a bizalmas adatokra viszonylag kevés nyilvános információ áll rendelkezésre, de az elemzés kiemeli a tévedésből eredő adattovábbítás jelentőségét, amikor például érzékeny információk rossz címzetthez kerülnek, de nagy problémát okoz a papír alapú dokumentumok tömeges postázása, a boríték és a benne lévő tartalom különbözősége, a címzettek és küldemények felcserélése. A kifinomult támadási praktikák és ezt követő jogsértés kevésbé ismert a vállalatok vagy szervezetek számára. Ezt igazolja az ENISA szervezet által kiadott *Data Breach 2019-2020*. évi összefoglalója, amely az összegyűjtött incidensek adatainak átfogó dokumentuma[246]. Az ENISA szakértői megállapították, hogy minden kockázat ellenére a szervezetek évről-évre egyre több adatot tárolnak az úgynevezett felhő infrastruktúrákban. A felhő megoldások előtérbe helyezését a helyi üzemeltetéssel szemben, a megfelelő technikai és biztonsági szinttel rendelkező informatikai infrastruktúra iránti igény, a kivitelezés és a dinamikus technológiai fejlődés lekövetése indokolja. Általában megállapítható, hogy a szervezetek kevésbé tudják, hogy a tárhely szolgáltatók helyileg hol, mely földrészen vagy országban tárolják az adatokat, és valójában milyen adatmentési műveleteket hajtanak végre. Természetesen a szolgáltató információbiztonsági tanúsítványa és besorolása garancia lehet az ügyfél számára, de teljes mértékű információbiztonság nem létezik, némi maradványkockázat mindig van. Véleményem szerint az ügyfél ki vannak téve az ismeretlen struktúrával rendelkező környezetnek, ami az adattárolásra nézve kockázattal jár. A tanulmány szerint a 2019-2020. évben az adatvédelmi incidensek számának növekedése is ezt igazolja. Az ENISA felmérése szerint 2019-2020. évben a korábbi évhez viszonyítva 54%-kal nőtt az adatvédelmi jogsértések száma, az adatvédelmi incidensek 71%-ának oka a pénzügyi motiváció, ebből 25% a kémkedés, az incidensek 32%-a adathalászat volt. A felmérés rávilágít arra, hogy az e-mail típusú adathalászat egyben az egyik legfontosabb rosszindulatú programok szállítási módja is, ami

[246] ENISA Threat Landscape 2020 - Data Breach, October 20, 2020

összesen 94% volt. Az adatvédelmi incidensek 52%-a hacker tevékenység, ebből a 33% az úgynevezett „*social attacks*”, 28% „*malware*” és 21% hibás kód alapú támadás volt. Ugyanez a hacker típusú támadás 2019. évben közel 59%-os volt. 70% adatszivárgás során email-en beszerzett felhasználói név és jelszó párosra koncentráltak az elkövetők, és a megkérdezettek csupán 55%-a aggódik az miatt, hogy a csalók vagy a bűnözők hozzáférnek a személyes adataikhoz, ami szerintem aggasztó és a ismerethiányra utal. A kutatói adatokkal is megerősítették álláspontomat, miszerint elég egyetlen téves informatikai konfigurálás, és a teljes adatbázis nyilvánossá válik, az adatok kereshetősége pedig komoly adatvédelmi incidenshez vezethet. A legtöbb adatszegés a felhőben az emberi mulasztásnak, a téves konfigurációnak köszönhető, de általában a szándékosság mértéke csekély, ugyanakkor a rendszerhiba vagy az emberi mulasztás által okozott kár költsége magas, 3,24 millió USD (2,4 millió EUR) volt. Felmérésem alapján megállapítható, hogy az adatvédelmi költséggel már nagyobb szervezet vagy vállalkozás esetében (világviszonylatban legalább 25.000 alkalmazott) mindenképpen számolnak, ami alkalmazottanként 204 USD (173 EUR) összegbe kerül a szervezetnek, a teljes becsült összeg 5,11 millió USD (ami 4,33 millió EUR átszámolva). Kisvállalkozások (500-1000 alkalmazott) esetében az adatvédelem átlagos költsége 3533 USD (3 000 EUR) alkalmazottanként számolva, a teljes költség pedig 2,65 millió USD (2,24 millió EUR) évente. A hacker tevékenységek motivációi között első helyen áll a pénzügyi haszonszerzés és a személyes adatok megszerzésének indítéka, és csak ezt követi a kémkedés. A statisztikai adatok alapján megállapítottam, hogy célpont szempontjából az egészségügy továbbra is az egyik legvonzóbb a kiberbűnözők számára és a *Ransomware* nevű zsarolóprogram, valamint a különféle adathalász technikák voltak a legnépszerűbbek. Esetenként több millió euró költségbe is belekerült a helyreállítás vagy a váltságdíj. 2019-ben 400 egészségügyi intézmény jelzett adatsértést, vagy adatszivárgást a betegeinek adataival kapcsolatban. Az adatvesztés típusainál az e-mail és a gyenge jelszavas hozzáférések általi adathalászat a legnépszerűbb (Adatípus adatszivárgás során, ENISA felmérés, 2019-2020.). A 2019. évi kutatási eredmények alapján megállapítottam, hogy az állami, az egészségügyi és a pénzügyi szektort ért hackertámadás, adathalászat és adatvesztés jelentősebb, mint a többi ágazatban vagy szektorban. A felmérések arra is rámutatnak, hogy egészségügyi adatokkal való visszaélés riasztó mértékben növekszik. Több egészségügyi intézmény, többek között 2016-ban egy magyar kórház informatikai rendszere is áldozatává vált az e-mailen keresztül, az intézmény információs rendszerébe bejutó zsarolóvírus által. A kórház teljes informatikai hálózatát leállították a helyreállítás végéig. A vírus által okozott adatvesztés mértékét, és a teljes

kárt nehéz megállapítani Abban az esetben, ha az adatok nyilvánossá válnak, valószínűsíthető az adatvesztés mértéke. A brit egészségügyi rendszert ért 2017. évi WannaCry támadás az Egyesült Királyságnak 92 millió fontba került. A támadás eredményeként több ezer ellátást, háziorvosi időpontot és műtétet kellett törölni, a sürgősségi ellátásokat átirányították más, zsarolóvírussal nem érintett intézményekbe. Tényleges adatvesztésre vonatkozó információval nem rendelkeznek, mivel az elsődleges céljuk a helyreállításra összpontosult, és váltságdíjat nem szándékoztak fizetni. A felmérések szerint globálisan több, mint 100 országban 200.000 számítógépet sújtott a zsarolóvírus.[247] Bár a publikus felmérések nem foglalkoztak a vírus útjára bocsájtásának kiváltó okával vagy annak céljával, mégis érdemes lenne a vizsgálatokat folytatni arra vonatkozóan, hogy csupán váltságdíj, vagy az illegális adatszerzés és adatbányászat áll a támadás hátterében. Amennyiben az utóbbi eset is fennáll, az esetlegesen megszerzett egészségügyi adatokkal tekintélyes mértékű visszaéléseket lehet végrehajtani, akár a mesterséges intelligenciával együttesen. A felmérések alapján további megállapításaim szerint a számítógépes támadási típusok (jogsértések, ENISA felmérés, 2019-2020.) között ragsor is felállítható, amely szerint sorrendben a következő lehet adathalászat e-mailen keresztül, amelynek 40%-a az egészségügyi ágazatot érinti, illetve felhőben tárolt vagy weboldal alkalmazások hitelesítő adatainak megszerzésére irányuló illegális tevékenység, amely lehet a kiszolgáló gyengeségeinek kihasználása vagy információlopó, rosszindulatú programok futtatásának alkalmazása, továbbá emberi mulasztás okozta sérülékenység, elsődlegesen konfigurációs hibák vagy biztonsági rések kihasználása. Az előbb felsorakoztatott érvek szerintem azt igazolják, hogy az adatvédelem jelentősége nem megkérdőjelezhető. A felmérések azt is igazolják, hogy az összes adatvesztés hátterében emberi tevékenység, jórészt hiszékenység vagy mulasztás áll, ami a támadás során, mintegy gyenge láncszem kihasználható. Tekintettel az emberi tényezőre a jogalkotók már a számítógépes alkalmazások és kommunikációs lehetőségek megjelenése és tömeges használata előtt adatvédelmi alapelveket és szabályokat állítottak fel, amelyek egyaránt a papír és az elektronikus személyes adatok védelmét szolgálja.

[247] National Audit Office, Investigation: WannaCry cyber attack and the NHS, by the Comptroller and Auditor General, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf, letöltés: 2021. április 3.

3.2. A HAZAI ADATVÉDELMI ELJÁRÁSOK ÉS STATISZTIKAI ADATOK VIZSGÁLATA

Amennyiben hazai területen szeretnénk megvizsgálni az adatvédelmi incidenseket és védekezéseket, valamint az indított ügyekhez kapcsolódó jogi állásfoglalásokat, határozatokat, valamint technikai ajánlásokat, úgy a már korábban említett két hatóság segít az ügyek értelmezésében és a statisztikai adatok elemzésében, a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) és a Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet (NBSZ NKI). A NAIH-hoz beérkezett ügyek és a Hatóság által évenkénti rendszerességgel megjelentetett beszámolója[248] alapján megállapítható, hogy évről-évre növekszik az esetek száma, mind határon innen, mind pedig határon túlról, az EGT tagállamokból érkezők[249] vonatkozásában. A Hatósághoz 2020-ban 784 ügy érkezett a Belső Piaci Információs Rendszeren (a továbbiakban IMI rendszer) keresztül, amelynek hozzávetőleg 25%-ban volt érintett. Ebből 2020-ban a Hatóság 11 eljárásban szerepelt fő felügyeleti hatóságként és 15 saját eljárást indított (GDPR 56. cikk szerint), továbbá 86 vizsgálandó döntéstervezet, 16 felülvizsgált döntéstervezet, és 97 jogerős döntés érkezett be, valamint 98 együttműködést segítő informális konzultációt fogadott (GDPR 60. cikk szerint), egyúttal. 4 kölcsönös segítségnyújtási eljárás és 111 önkéntes kölcsönös segítségnyújtási kérelem érkezett, valamint 7 kölcsönös segítségnyújtási eljárást, és 12 önkéntes kölcsönös segítségnyújtási eljárás kezdeményezett. A NAIH ügyeinek száma különböző típusonként csoportosíthatók. A GDPR 2016. május 24-én hatályba lépést követő kétéves türelmi időszak után, tehát a 2018. május 25-től kötelezően alkalmazandó, legfőképp a GDPR és az Infotv. rendelkezésekhez kapcsolódó ügyek esetében, és az általam vizsgált NAIH által nyilvánossá tett határozatok, és a határozatok ügytípusai által összeállított statisztikai adatok szerint 2018 - 2020. évekre vonatkozóan a további következtetéseket vontam le. Az adatvédelmi konzultáció, állásfoglalás iránti kérelem ügykör ügyszáma fokozatosan csökkenő tendenciát mutat, 29%-kal csökkent, ami valószínűleg az új rendelkezések szélesebb körű elfogadására és alkalmazására utal. Adatvédelmi szempontból tudatosabb felhasználásra utal az információs rendszereket, weboldalakat, webkamerákat napi szinten alkalmazók körében. Az adatvédelmi ügyben lefolytatott vizsgálati eljárás erős növekedést mutat, ami igazolja az előző megállapítást, hiszen a biztonságtudatos

[248] A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2021. évi tevékenységéről, (B/18074) Nemzeti Adatvédelmi és Információszabadság Hatóság Budapest, 2022.
[249] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), A Nemzeti Adatvédelmi és Információszabadság Hatóság 2020. évi beszámolója, VII. Nemzetközi ügyek és társadalmi kapcsolatok,164.o., https://www.naih.hu/eves-beszamolok, letöltés: 2021. április 3.

attitűddel rendelkező felhasználók a felhasználói közösség többi tagját is az adatvédelmi szabályok betartására ösztönöznek, kéréssel vagy eredménytelen felszólítás esetén a NAIH felé benyújtott panasszal. Az esetek közé tartozik a vélt, vagy valós sérelmen alapuló panaszos ügyekben lefolytatott adatvédelmi vizsgálati eljárás és a hatósági határozatok alapján megállapítható, hogy minden esetben a Hatóság igyekszik a törvényes keretek között, hivatalosan, de köznapi szóhasználattal élve humánusan rendezni a vitás ügyleteket. Ez utóbbi megállapítás azzal igazolható, hogy a Hatóság csak indokolt esetben állapít meg adatvédelmi bírságot, egyes ügyekben elegendő volt a figyelmeztetés, de a kötelezés vagy a felszólítás eseteiben gyakori már az adatvédelmi bírság megállapítása is. Ezen ügyek, illetve a nyilvános határozatok statisztikái adatelemzésemre ebben a fejezetben bővebben ki fogok térni. Az adatvédelmi vizsgálati eljárások számának vizsgálata szerint, míg 2019-ben 1738 adatvédelmi vizsgálati eljárást rögzítettek, 2020-ban elérte a 2400 eljárás számát, ami az előző évhez képest 38,1%-os növekedést jelent. 2020. évi ügyszám háromszorosa a 2018. évihez képest, 2016. évhez viszonyítva pedig négyszeres emelkedést jelentett. Az ügyszámok tükrözik az adatvédelmi ügyek meredeken felfelé ívelő gyarapodását. A hatósági eljárások tekintetében az adatvédelmi ügyekben a GDPR terület (2019-ben: 1572, 2020-ban: 2044 ügy), az adatvédelmi incidens, a bűnüldözést érintő ügyek a legjelentősebbek. Az információszabadság tekintetében lefolytatott vizsgálati eljárás 2019. évben 325, 2020. évében pedig 538 eljárást kezeltek, ami 65,5%-os emelkedés, ami az elmúlt öt évre nézve a legnagyobb éves szintű növekedést jelent. Korábbi évekkel összehasonlítva a változás 10-65,5% közötti növekvő tendenciát mutat[250]. Az adatvédelmi hatósági eljárások, valamint a hatósági ellenőrzések száma szintén növekszik, ami arra utal, hogy egyes vállalkozások, szervezetek figyelmen kívül hagyják az Infotv. rendelkezéseit, elmulasztják az adatvédelmi tájékoztatási kötelezettséget, sérül az adattakarékosság, az átláthatóság vagy a célhoz kötöttség elve, és esetenként még a hatósági felszólításra sem tesznek eleget adatvédelmi kötelezettségeiknek. A NAIH ügyköreire vonatkozó részletesebb adatokat az alábbi táblázat mutatja, a folyamatban lévő ügyek 32%-os, az éves ügyszám, beleszámítva a DPO ügyeket, pedig 44%-os növekedést mutat. Az ügyszám növekedés nemcsak az adatvédelmi incidensek növekedésére, de az adatvédelem jelentőségére, és mint hatósági ügyek gyarapodására, valamint az indokolt adatvédelmi ellenőrzések lefolytatására is utal. A NAIH az adatvédelmi irányelveknek megfelelően őrködik, különösen a személyes adatok törvényes kezelése, feldolgozása, továbbítása fölött, nemcsak hatósági ellenőrzést folytat vagy adatvédelmi incidenst vizsgál ki, hanem állásfoglalásokkal segíti a

[250] NAIH 2020. évi beszámolója, Vizsgálati eljárások száma: 2016-2020. alapján

vállalkozások, az intézmények és a magánszemélyek eligazodását a GDPR és az Infotv. számukra ismeretlen területén. Bár az adatvédelmi konzultáció és állásfoglalás kérelmének száma 2018. év óta csökken, így 2409 ügyről 1710-re, de az ügyszám mértéke így is számottevő.[251] A vállalkozásokat és az intézményeket elsődlegesen az adatvédelmi szabályozás legmegfelelőbb rögzítése és a gyakorlati megoldás vezeti az állásfoglalás kérésére. Az ügyeket tekintve csökkenő tendenciát mutat a jogszabályvéleményezés is, ami véleményem szerint a GDPR és az Infotv. rendelkezések megfelelően széles körű és részletes, a Hatóság által támogatott, és rendszeresen megtartott adatvédelmi konferenciáknak, a Hatóság által kiadott állásfoglalásoknak és nyilvános tájékoztatóknak, valamint a rendszeresen lebonyolított DPO képzéseknek köszönhető. A GDPR és az Infotv. tartalmazza mindazon jelentős, az 1980-ban a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Irányelvében, valamint az Európa Tanács 1981. január 28-i 108. számú, az egyéneknek a személyes adataik gépi feldolgozása során való védelméről szóló egyezményben foglaltakat, valamint a társadalmi és technikai fejlődés által eredményezett további irányelveket és rendelkezéseket. Tehát a rendelkezésekbe belekerült különösen az adattakarékosság[252], a „*privacy by default*”, vagy a „*privacy by design*” [253] elve. A Covid-19 vírus által okozott világjárvány előtérbe hozta a privát kamerák mindennapos használatát az online oktatás és tanulás, távmunkavégzés teljesítés során.

A NAIH által közzétett NAIH/2020/7127 ügyszámú a digitális távoktatás adatvédelmi és adatbiztonsági vonatkozásairól szóló tájékoztatója véleményem szerint segíti az online oktatás törvény szerinti megvalósítását, így például az oktatók és diákok kamerahasználata során jogszerűen kezelhető adattartalomra és az adattakarékosság elvére is felhívja a figyelmet. Azokon a távoktatásokon ahol a kamera használata elengedhetetlen, szükséges meghatározni a kamerahasználat célját, valamint a felvételek tárolásának módját, mint információbiztonsági követelmény és idejét, mint adatvédelmi előírás. A kamerahasználat esetenként eltérő lehet, ezért a meghatározása egyedi elbírálás alapján lehetséges. A digitális távoktatás során is figyelembe kell venni a személyes adatok kezelésére vonatkozó előírásokat, így különösen azon képi, hangi és videofelvételekre vonatkozókat, amelyek tartalmazzák a diák vagy az oktató személyével kapcsolatos információkat. Az oktatás keretein belül keletkezett személyes adat,

[251] NAIH 2020. évi beszámolója, hatósági ügyek száma 2018-2020.
[252] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR) 5. cikk A személyes adatok kezelésére vonatkozó elvek (1) bek. c), „a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”)”.
[253] Nemzeti Adatvédelmi és Információszabadság Hatóság, https://naih.hu/adatvedelmi-szotar, letöltés: 2021. március 20.

így az online vizsgáztatás vagy feleltetés, a tanár-diák konzultáció, vagy az oktatást-tanulást segítő chat nem minősül magáncélú adatnak és kezelésnek célja a törvényben meghatározott közfeladat ellátása, illetve annak folytonosságának fenntartása. Az adatkezelő ebben az esetben nem a pedagógus vagy az oktató[254], hanem a tankerület vagy az adott oktatási intézmény, és az adatkezelő kötelezettsége és felelőssége az oktatáshoz szükséges megfelelő technológia kiválasztása, használatának engedélyezése valamint ellenőrzése.[255] Az előbbieken túl a digitális oktatásban résztvevőkre, így különösen az oktatókra és pedagógusokra vonatkozik a titoktartási kötelezettség. A virtuális tért úgy kell tekinteni, mint az oktatótermet vagy az osztálytermet, ahol ugyanúgy nem megengedett az oktatási tevékenységet nem szolgáló, felesleges képi és hangfelvétel rögzítése. Az előadások, akár online vagy jelenléti, védett tartalomnak minősülnek, így azok jogtalan felhasználása szerzői jogi, adatvédelmi jogi és esetleges büntetőjogi jogkövetkezményt vonhat maga után, ami nemcsak az oktatóra, a pedagógusra, a szülőkre, de azokra a diákokra is érvényesíthető, akik betöltötték a 18. életévüket. A digitális távoktatás során keletkezett személyes adatokat tartalmazó digitális információk kezelésére és tárolására is érvényesíteni kell az adattakarékosság elvét. Tehát az online oktatás során kerülni kell a felesleges, különösen a magánszféra környezetét rögzítő tevékenységeket. Abban az esetben, ha mégis szükséges és az oktatást illetve a tanulás elengedhetetlen részét képezi a tanórához vagy előadáshoz kapcsolódó, személyes adatokat tartalmazó, képi, videó vagy hangfelvétel tárolása és kezelése, úgy azok kezelésénél és feldolgozásánál a korlátozott tárolhatóság elvének teljesíthetőségét figyelembe kell venni. Tehát ezeket a digitális tartalmakat csak a meghatározott mértékig, a szükséges időtartamig lehet felhasználni és tárolni. Különbséget kell tenni hivatali feladatokat ellátó, jogszerű adatgyűjtés és kényelmi szempontokat támogató adatbázis építés és kezelés között. Személyes adatokat gyűjteni kizárólag indokolt, törvényi előírásoknak megfelelően és azok teljesítésének céljából lehetséges. Tehát például kollégium, munkásszálló vagy egyéb szállást és ellátást biztosító intézmény folyosóján elhelyezett, biztonsági és védelmi célokat szolgáló kamerafelvételek tárolása, kezelése a megengedett időtartamig lehetséges és szükségszerű, de a zuhanyzóban vagy hálószobában elhelyezett kamera és a felvételeinek tárolása személyiségi jogokat sért,

[254] Nemzeti Adatvédelmi és Információszabadság Hatóság, Ügyszám: NAIH/2020/7127/ Tájékoztató a digitális távoktatás adatvédelmi és adatbiztonsági vonatkozásairól, III.5.

[255] Nemzeti Adatvédelmi és Információszabadság Hatóság, Ügyszám: NAIH-3706-2/2021, Állásfoglalás a digitális távoktatás keretében a tankerületi igazgató, mint munkáltató és a pedagógus, mint foglalkoztatott között megköthető, a munkáltató által a munkavégzéshez biztosított, valamint a saját információtechnológiai vagy számítástechnikai eszközök, rendszerek használatáról szóló megállapodás adatvédelmi és adatbiztonsági vonatkozásairól, II.

kivéve, ha az szerződésben rögzített módon, a megfigyelt személy hozzájárulásával (valóság show) vagy kifejezett személyi védelmére, őrzésére történik (börtön). Ha a kollégiumi elhelyezés nyilvántartási kötelezettségéből adódóan szükséges a hallgatók személyes adatainak rögzítése és kezelése, beleértve a hallgatók közösségi térben való mozgásának felügyelete, akkor az adatkezelés, tehát az adattárolás és -kezelés a szükséges időtartamra nézve jogszerű, például a hallgató kollégiumi ellátásra való jelentkezésétől, a kollégiumi szobájának átadásáig és a kollégium elhagyásáig történő időszakra vonatkozóan. Ugyanakkor, ha a kollégium rendszergazdája ideiglenesen, saját célból menti, másolja, vagy tárolja a hallgatói személyes adatokat tartalmazó nyilvántartást, akkor már nem jogszerű és a tevékenység szankcionálható. Továbbá az intézményi felelősségen túl a munkavállalói felelősséget is érinti, mivel nemcsak jogszerűtlen az adatkezelés, de az adott intézmény biztonsági adatmentésre vonatkozó előírásait sem tartja be. Amennyiben a rendszergazda haszonszerzés céljából tárolta a hallgatói adatbázist és ez bizonyítható, úgy büntetőjogi felelősségre is vonható. A nem megengedett tevékenység gyakorlása esetén az információbiztonsági előírások, úgymint a hozzáférés szabályai is sérülnek, hiszen önmagában az a tény, hogy egy intézmény rendszergazdája a személyes adatokat tartalmazó adatbázisszerver biztonságos működéséért felel, nem jelenti azt, hogy az adatbázisban tárolt személyes vagy szervezeti, ipari, illetve gazdasági adatokat megtekintheti, kezelheti vagy feldolgozhatja. Az ipari, legfőképp kísérleti, egyéb technológiai adatok megszerzése, jogosulatlan felhasználása vagy továbbítása az ipari kémkedés kategóriába, a szervezet pénzügyi adatainak jogosulatlan megszerzése és felhasználása, azzal való károkozás, gazdasági adatokkal való visszaélés, valamint esetlegesen gazdasági bűncselekmény, míg a jogtalan személyes adat kezelése, személyes adattal való visszaélés kategóriájába tartozhat. Mindez abban az esetben áll fenn, ha a vonatkozó jogszabályi előírások és a jelentős érdeksérelem megvalósulása között ok-okozati összefüggés bizonyítható[256], és a rendelkezések megsértése a Btk.-ban meghatározott módon valósult meg. Az ok-okozat összefüggések megállapíthatósága esetenként egyedi lehet, ezért csak rendkívül alapos felméréssel lehet az eredményt meghatározni. Például, ha egy feltételezett adatvédelmi incidens során, azért váltak az intézmény kezelésében lévő személyes adatok nyilvánossá az interneten, mert a rendszergazda azokat nem megengedett helyen, ideiglenesen és védelmi előírásokat figyelmen kívül tárolta, de a rendszergazdának az adott intézménnyel semmilyen megállapodása nem volt

[256] Péterfalvi Attila, Eszteri Dániel (2017) A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata. In: A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. ELTE Állam- és Jogtudományi Kar, Budapest, pp. 405-420., http://real.mtak.hu/97033/, letöltés: 2021. április 17.

arra vonatkozóan, hogy az adatokat bármilyen módon kezelheti, úgy nehezen állapítható meg az ok-okozati összefüggés és a felelősség. Az adatvédelem tekintetében kiemelten fontos, hogy a helyi szintű adatvédelmi szabályozás ne csak tükrözze a törvényi előírásokat, de összhangban legyen a gyakorlati megvalósítással is és a személyes adatokat kezelők feladatköreinek és a felelősségeinek meghatározásával. Az adatvédelmi és az információbiztonsági előírás szerinti személyes adatokhoz való hozzáférés megfelelő szabályozása és gyakorlati alkalmazása indokolttá teszi a különböző jogosultsági szintek létrehozását és elszeparálását. A rendszerüzemeltetői szinten is tudatosítani kell a jogszabályi, adatvédelmi, információbiztonsági alapelveket, így nemcsak a munkavállalói, de az adatvédelmi jogokat és kötelezettségeket. Amennyiben bármelyik alapelv betartása veszélybe kerül, a rendszerben sebezhetőség, gyenge pont keletkezik, amely a teljes információs rendszer működését veszélyezteti és nő az információbiztonsági kockázat. A fentiekből is látszik, hogy az adatvédelemi előírások és az adatbiztonsági követelmények nem teljesülésének több szintje is létezik és az adatvédelmi alapelvek eseteken, állásfoglalásokon, konferenciákon keresztül történő népszerűsítése ma már elengedhetetlen és rendkívül hasznos, mert az egyik mód arra vonatkozóan, hogyan lehet eligazodni a GDPR színes útvesztőiben és tartani az alapelvek útmutatásait. Az adatvédelmi állásfoglalásokat kiegészítik az adatvédelmi és információbiztonsági továbbképzések. Bár az adatvédelmi tisztviselő (DPO) képzéseket elsősorban jogász, míg az információbiztonsági vezető (információbiztonsági felelős, IBF) képzéseket[257], informatikus mérnök szakképzettséggel rendelkezők számára ajánlják, gyakori az áthallgatás, tekintettel arra, hogy a két szak az adatvédelmi és az információbiztonsági közös témák terén szorosan kapcsolódik egymáshoz. Népszerű az adatvédelmi szaktanácsadó képzés[258] is, amely célja a GDPR előírásairól ne csak általános módon, hanem átfogóbb, gyakorlati ismereteket szerezhessenek, de megfelelően alkalmazni is tudják a rendelkezéseket az adatvédelmi szabályrendszer ismeretén keresztül. A szakképzések jelentősen segítik az adatvédelmi és információbiztonsági alapelvek és előírások teljesíthetőségét, a törvények, rendelkezések és intézményi előírások megértését, elfogadását és gyakorlati alkalmazását.

[257] Nemzeti Közszolgálati Egyetem, Elektronikus információbiztonsági vezető szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok, letöltés: 2021. április 14.

[258] Nemzeti Közszolgálati Egyetem, Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok, letöltés: 2021. április 14.

3.2.1. ADATVÉDELMI ELJÁRÁSOK

A NAIH statisztikai adatai közül kiemelendő azon adatvédelmi ügyben lefolytatott vizsgálati eljárás statisztikai adatai, amelyek a Hatóság által nyilvánosságra hozott határozatok adatait, kategóriáit tartalmazza. Saját kutatás keretében vizsgáltam a 2019. évi 48, 2020. évi 47, valamint 2021. évi 29 a NAIH által nyilvánossá tett, anonim vagy részben publikus adatokat tartalmazó határozatokat, abban foglalt eseteket, eljárásokat. A hatóság által nyilvánosan közzétett határozatokból származó kutatási eredményemként előállt és elemzett statisztika kimutatásból megállapítható, hogy a hivatalból, valamint a kérelemre indított vizsgálati eljárások száma, egymáshoz viszonyított aránya csak kis mértékben emelkedett 2019. és 2020. években (26%-ról 33%-ra), míg 2020. évhez képest 2021-ben jelentősen csökkent (21%-ra). A kérelemre indult vizsgálat lényegesen meghaladta a hivatalból indítottak számát, ami 2021-ben már 83% volt. Tehát megállapítható, hogy 2021-ben nyilvánosságra hozott határozatok tekintetében a Hatóság kérelemre indított eljárás keretében 4-szer annyi esetben járt el, mint a hivatalból indított esetekben. A NAIH az érintett személyes adatok védelméhez való jog érvényesülése érdekében, kérelmére adatvédelmi hatósági eljárást indíthat. Amennyiben az érintett panasszal élne a vélt vagy valós jogsértés ellen és hatósági eljárás keretében történő kivizsgálást kíván, a kérelmének meg kell felelnie formai és tartalmi követelményeknek is. A kérelmet az érintettnek írásban, papíron vagy elektronikus formában[259] kell benyújtania és a beterjesztett nyilatkozatában egyértelműen, meghatározott módon kell kérnie a hatósági eljárás lefolytatását, illetve a hatóság döntését és a jogos érdek érvényesítését. Az Infotv. alapján a kérelemnek tartalmaznia kell az érintett kérelmező, valamint jogi képviselője azonosításához, kapcsolattartáshoz szükséges adatokat, a feltételezett jogsértés megnevezése és az eset vagy állapot részletes leírását, az érintett adatkezelő, vagy adatfeldolgozó megnevezése és az azonosításhoz szükséges adatokat, a feltételezett jogsértéssel kapcsolatos állításokat alátámasztó tényeket és bizonyítékokat, valamint a jogsértésre vonatkozó határozott kérelmet.

Amennyiben a kérelem az Infotv. szerinti kötelező tartalmi elemeket nem tartalmazza, és a kérelmező a hiánypótlásnak sem tesz eleget, a Hatóság a kérelemre indított eljárást megszünteti vagy visszautasítja. A Hatóság csak azokat az adatkezelésre vonatkozó sérelmet tartalmazó kérelmeket fogadhatja be, amelyek 2018. május 25-e, az Infotv. vonatkozó rendelkezéseinek hatályba lépése után keletkeztek. Kérelemre vagy hivatalból induló eljárás esetén a NAIH azonosítja a kérelmezett adatkezelőt vagy adatfeldolgozót, megvizsgálja az illetékességet, tehát

[259] NAIH Online Ügyindítás, Online ügyinditás - e-Papír

az ügy határon belüli vagy határokon átnyúló érintettségét. Amennyiben határokon átnyúló illetékességű, akkor megállapítja, hogy mely uniós tagállam adatvédelmi hatósága az érintett. A NAIH hivatalból indított hatósági eljárásainak előzménye az esetlegesen hivatalból induló hatósági ellenőrzés. Amennyiben hivatalból indult a hatósági ellenőrzés, a Hatóság az ellenőrzésről jegyzőkönyvet készít. Ha a jegyzőkönyvben jogsértést állapít meg, és hatósági érdemi döntés születik, az érintett felet tájékoztatja. A döntés feltételeinek hiányában adatvédelmi hatósági eljárás indul. A vizsgálati eljárás követően a Hatóság adatvédelmi hatósági eljárást indít abban az esetben, ha a jogsérelem orvoslása vagy közvetlen veszélyének elhárítása nem történt meg, a Hatóság megállapította, hogy a személyes adatok kezelésével kapcsolatban jogsérelem következett be és indokolt a bírság kiszabása, a Hatósági ellenőrzés jogsértést tárt fel, illetve közérdekű bejelentés, hivatali észlelés, vagy más hatóságok tájékoztatása alapján indokolt. A Hatóság által nyilvánossá tett dokumentumok (határozatok, beszámolók) vizsgálata alapján megállapítottam, hogy a határozatok az eljárásokhoz viszonyított aránya, hivatalból indult eljárások esetében 2019. évben 26%, 2020. évben 33%, 2021. évben 21%, míg a kérelemre indult eljárások esetében 2019. évben 74%, 2020. évben 67%, 2021. évben 83% volt. A kérelemre indult esetek tekintetében az eljárások száma növekvő tendenciát mutat. A vizsgált, 2020., valamint 2021. évi határozatok között csupán egy-egy olyan megállapítás volt, amelynek eljárása kérelemre és hivatalból is indult. A határozatban rögzítettek alapján az internetes kereső olyan hirdetéseket jelenített, meg amely alapján a kérelmező azt feltételezte, hogy a nevét összekapcsoltan kezelik a szakmájával és automatikus döntéshozatali eljárásokban használják fel, tehát az internetes kereső profilozásra utaló tevékenységet folytat. A kérelmező felszólítására a kérelmezett nem tudott segíteni, ezért a Hatósághoz fordult és kérte az ügy kivizsgálását, a kérelmezett érintetti jogokkal összefüggő gyakorlatának vizsgálatát, az adatkezelő elmarasztalását és a kért tájékoztatásra vonatkozó kötelezését.[260] Tekintettel az ügyben megfogalmazott adatkezelés határokon átnyúló jellegére a Hatóság az általános adatvédelmi rendelet 56. cikke szerinti eljárás lefolytatásának érdekében az ír adatvédelmi hatósághoz, mint főhatósághoz fordult, amely tájékoztatása értelmében a

[260] „*A Kérelmezett álláspontjával szemben a Hatóság álláspontja szerint a Hatóság az általános adatvédelmi rendelet 56. cikke szerinti eljárás eredményeképpen a főhatóságként azonosított ír adatvédelmi hatósággal egyetértésben jogosult a kérelmet kivizsgálni, és a tényállást teljes körűen feltárni. … A Hatóság annyiban vizsgálta csak a Kérelmezett általános gyakorlatát, amennyiben az kihatással van a Magyarországon tartózkodó érintettek érintetti jogai gyakorlásával, valamint annak megállapításához szükséges, hogy indokolt-e az ír adatvédelmi hatóság mint főhatóság megkeresése eljárás indítása céljából.*”
Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: kérelemnek részben helyt adó határozat, hivatalbóli eljárást megszüntető határozat, jogsértés megállapítása Iktatószám: NAIH/2020/5553, korábbi ügyszám: NAIH/2019/346

Hatóság helyi ügyként kezelhette az esetet. A Hatóság megállapította, hogy a kérelmezett magatartása megsértette az általános adatvédelmi rendelet 12. cikk (3) bekezdését és 15. cikk (1) bekezdését, viszont a kérelmezett időközben teljesítette a tájékoztatási kötelezettségét, tehát teljesítésére kötelezése az eljárás során okafogyottá vált. A hivatalból indított hatósági eljárás tovább folytatása nem volt indokolt, mivel a rendelkezésre álló információk alapján a kérelmezett általános gyakorlatával kapcsolatban jogsértésekre nem merült fel bizonyíték. A következő, az adatvédelmi jogsértésekhez kapcsolódó, vizsgált ügy, egy adatfeldolgozást érintő adatvédelmi incidenssel kapcsolatos, amely esetben a hatósági ellenőrzés során feltárt körülmények miatt indított a Hatóság hivatalból adatvédelmi hatósági eljárást. A Hatósághoz közérdekű bejelentés érkezett, amely arra hívta fel a figyelmet, hogy egy utazási iroda weboldalán keresztül bárki számára elérhetőek az ügyfelek személyes adatai, így többek között az utasok neve, elérhetőségei, lakcímadatai, valamint személyi igazolvány és útlevélszámok, és a foglalással, utazással, úticéllal, szállással valamint a szerződéskötéssel kapcsolatos adatok.[261] Az incidenst egy fejlesztés alatt álló weboldal tesztkörnyezetében található, de valós személyek adatait is tartalmazó adatbázisának nyilvánossá tétele, illetve megfelelő védelem nélküli használata, fejlesztése váltotta ki. A sérülékenység összesen 781 természetes személy személyes adatát, többek között kiskorú személyek adatát érintette, közel 2500 rekordot. Az adatvédelmi incidenssel kapcsolatos személyes adatok kezelése az adatok jellegéből fakadóan magas kockázattal járt, magas fokú biztonsági intézkedést igényelt volna. Az eset hivatalból indított hatósági eljárás következménye többek között az adatvédelmi bírság megállapítása. A Hatóság kérelemre indított esetei között példaként említendő a jegy- és bérletkiadó automatából egy havi bérletszelvény vásárlásának esetével foglalkozó ügy. A határozat értelmében a Hatóság részben helyt adott a kérelmező kérelmének, mivel megállapította, hogy a kérelmezett nem tájékoztatta a kérelmezőt a róla kezelt személyes adatairól és az adatkezelés rá vonatkozó információiról és nem teljesítette a kérelmező adatkezelés korlátozása iránti kérelmét. A Hatóság az eljárás során megvizsgálta többek között az adatkezelő és az adatfeldolgozó személyét, majd a kérelmező alábbi jogait, úgymint hozzáférési jog, korlátozáshoz való jog, és

[261] „*A letölthető szerződések részletesen tartalmazták valamennyi szerződő utas személyes adatait, az úticélt, az utazás dátumát, a lefoglalt szállás adatait és a szolgáltatás bruttó árát személyekre bontva.*
A Hatóság a fentiekre tekintettel hatósági ellenőrzést indított 2020. január 30-án, mivel a rendelkezésre álló adatok nem voltak elegendőek annak megítéléséhez, hogy Ügyfél 1. maradéktalanul eleget tett-e az általános adatvédelmi rendeletben foglalt kötelezettségeinek, így különösen a 32-34. cikkében foglaltaknak."
Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban Ügyszám: NAIH/2020/66/21

az eljárást részben megszűntette, valamint megállapította a szankcionálásra vonatkozókat.[262] Az említett esetekből jól látható, hogy a Hatóság a GDPR iránymutatás alapján, az Infotv. által felhatalmazott keretek között, egyben szem előtt tartva az Akr. előírásait[263], hatáskörében érdemben dönt és határozatot hoz a beterjesztett kérelmek és a hivatalból indított eljárások kapcsán, így szükség esetén a kérelemnek helyt ad vagy elutasítja, megállapít, figyelmeztet, felszólít vagy szankcionál. A szankcionálásnál figyelembe veszi a kötelezettségek teljesítését, a helyreállítást, a kár mértékét és jogi személy gazdasági, pénzügyi körülményeit is. Az esetek bővebb részletezése az adatvédelmi incidensek fejezetében találhatók, jelen részben csak a hivatalból vagy a kérelemre indított esetek elvi bemutatásának céljából rögzítettem.

3.2.2. AZ ADATKEZELÉS JOGSZERŰSÉGE

A jogalap és a jogos érdek kategóriáit tekintve a GDPR 6. cikke adhat választ a felmerülő kérdések tekintetében, legfőképp, hogy egy adatkezelés során mely esetekben lehet figyelembe venni a jogos érdeket.

Év / Megnevezés	2019. Határozatok száma összesen		2020. Határozatok száma összesen		2021. Határozatok száma összesen	
Vizsgált nyilvános határozat	**48**		**47**		**29**	
ebből:						
hivatalból indult	12	26%	15	33%	6	21%
kérelemre indult	35	74%	31	67%	24	83%
jogalap	17	36%	14	30%	17	59%
jogos érdek	5	11%	7	15%	7	24%
megállapítás	35	74%	40	87%	17	59%
figyelmeztetés	2	4%	6	13%	2	7%
felszólítás	9	19%	3	7%	0	0%
kötelezés	9	19%	14	30%	19	66%
végzés	11	23%	17	37%	3	10%
adatvédelmi bírság	27	57%	26	57%	14	48%

3. táblázat, A NAIH által nyilvánossá tett határozatai alapján készített statisztikai adatok, határozat típusok és döntések aránya, 2019-2021., saját adatgyűjtés és vizsgálat alapján

Amennyiben az adott vállalkozás vagy intézmény adatkezelőjének jogos érdeke, törvény által előírt kötelezettségének teljesítéséhez és feladatának elvégzéséhez elengedhetetlenül

[262] „*A Hatóság az Ákr. 47. § (1) bekezdés c) pontja alapján megszünteti az adatvédelmi hatósági eljárást a [Cég 2.] vonatkozásában, mivel a [Cég 2.] adatfeldolgozóként nem felel a jelen ügyben elkövetett jogsértésért, ezért az eljárás a [Cég 2.] vonatkozásában okafogyottá vált.*"
„*A Hatóság ugyanakkor hivatalból megvizsgálta, hogy indokolt-e a Kérelmezettel szemben adatvédelmi bírság kiszabása. E körben a Hatóság az általános adatvédelmi rendelet 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján mérlegelte az ügy összes körülményét és megállapította, hogy a jelen eljárás során feltárt jogsértések esetében a figyelmeztetés se nem arányos, se nem visszatartó erejű szankció, ezért bírság kiszabása szükséges*."
Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: Kérelemnek részben helyt adó határozat, Ügyszám: NAIH/2020/876/12. (NAIH/2019/8236.)
[263] 2016. évi CL. törvény, az általános közigazgatási rendtartásról, érvényben és hatályban: 2021. április 17.

szükséges, hogy a szervezetén belül belső adminisztratív célból személyes adatokat kezeljen és továbbítson, aminek részét képezi az ügyfeleinek (vevő, hallgató, diák és más természetes személy, akivel az ügy kapcsán hivatalból kapcsolatot tart) és az alkalmazottak személyes adatainak a kezelése és továbbítása, a tevékenység teljesítése jogos érdekből szükséges.

Az adatkezelés és adattovábbítás tevékenységbe beleértendő az adott vállalkozáscsoporton belüli, de harmadik országbeli telephely is. [264] A jogalap és a jogos érdek nem megfelelő hivatkozását mutatja például a NAIH/2020/3467. számú ügye, amely esetben az érintett Polgármesteri Hivatal nem a megfelelő jogalapra hivatkozott az ügy kivizsgálása során. Az adatkezelő felelőssége továbbá az adatkezelés céljának és jogos érdekének azonosítása és indoklása, amelynek részletes rögzítése elengedhetetlen, tehát adattípusra, és célszintre kell lebontani és szükségességét mérlegelni, indokolni, mindezt az adatkezelés megkezdése előtt szükséges elvégezni. Az adatkezelés jogszerűségének igazolása esetenként eltérő lehet. Például kamerás megfigyelések esetében az irodai munkakörnyezet, a benzinkúti értékesítés és a sportrendezvények megfigyelésének, valamint egy polgármesteri hivatal által elhelyezett térfigyelő kamera alkalmazásának célja, jogszerűsége és jogalapja is eltérő lehet. Egyes esetekben az adatkezelés többfajta célt is szolgál, ezért a biztonsági, a munkaügyi, a munkavédelmi, az egészségügyi valamint a bűnmegelőzési célok összefügghetnek. Többcélú adatkezelést szolgál a Covid-19 vírus által okozott világjárvány idején, a kórházakban, az oltási körülmények kialakítása és biztosítása, valamint megerősített kamerás információs rendszer alkalmazása. Véleményem szerint az egészségügyi intézményekben egyedi események során (mint például a tömeges oltás) indokolt lehet az élet és a testi épség védelme céljából is alkalmazott kamerás megfigyelés, mivel egyrészt munkaügyi célt szolgál, az egészségügyi dolgozók munkájának fokozottabb ellenőrzése által, másrészt egészségügyi célt szolgál, mert a

[264] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)
(47) „*Az adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait*."
(49) „*Az érintett adatkezelő jogos érdekének minősül a közhatalmi szervek, számítástechnikai vészhelyzetekre reagáló egység (CERT), hálózatbiztonsági incidenskezelő egységek (CSIRT), elektronikus hírközlési hálózatok üzemeltetői és szolgáltatások nyújtói, valamint biztonságtechnológiai szolgáltatók által végrehajtott olyan mértékű személyes adatkezelés, amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos, vagyis adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képessége az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek által nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben*."
6. cikk Az adatkezelés jogszerűsége

páciensek nyomon követésével, az egészségügyi állapotromlás esetén gyorsabb beavatkozás lehetséges, továbbá biztonsági célt szolgál, mert személyi védelem keretében védi az egészségügyi dolgozókat és a pácienseket az esetleges incidensek bekövetkezésétől. A fentiekből is látszik az egyértelmű következtetésem, miszerint a kamerás megfigyelés és összekapcsolása az információs rendszerrel több célú is lehet. Sok esetben idegenkedünk az alkalmazásuktól, a magánszféránk indokolatlan zavarásának tekintjük, és megfeledkezünk arról, hogy vagyon-, személy- és egészségvédelmi célzattal indokolt lehet a kialakítása és használata. Ugyanakkor a kamerás megfigyelőrendszer használata során különös tekintettel kell lenni a tájékoztatásra. Tehát a munkáltató a munkavállalót előzetesen, írásban tájékoztatni köteles a kamera által megfigyelt helyről. Az általános tájékoztatás itt nem elégséges. A munkáltató köteles továbbá a kamerás megfigyelőrendszerből származó adatokat jogszabályi előírásoknak megfelelően kezelni, tárolni és a szükségesség-arányosság elvét követni. A cél nélküli, indokolatlan megfigyelés nem megengedett tevékenység, továbbá a munkáltatónak igazolnia kell, hogy az alkalmazott kamerás megfigyelő- és információs rendszer teljesíti-e a célhoz kötöttség elvét az adatkezelés, adatfeldolgozás illetve az adattovábbítás során és az alkalmazása az adatkezelő jogos érdeke. Az adattakarékosság elve szerint a kamerarendszer kizárólag olyan területeket rögzíthet, ami a védendő vagyontárgyra vagy az ellenőrzendő területre vonatkozik. A kamerarendszerek felügyelete és adatkezelési, illetve adatfeldolgozói tevékenysége legtöbb esetben távoli hozzáféréssel történik, ezért ezen rendszerek működtetésénél az adatvédelmi előírásokat együtt kell alkalmazni az információbiztonsági előírásokkal. Az előírások nemcsak az alapelvek betartására vonatkoznak, de a technikai védelem kialakítását és működtetését, valamint az üzemeltető biztonságtudatos magatartását egyaránt érinti, úgymint információbiztonsági jogokra és kötelezettségekre vonatkozóan. Ezen megállapításaimat a NAIH vonatkozó határozatai és állásfoglalásai is megerősítik.

3.2.3. ADATVÉDELMI HATÁROZATOK ÉS INCIDENSEK STATISZTIKAI ADATAINAK VIZSGÁLATA

Az adatvédelmi incidensek és határozatok vizsgálata alapján megállapítottam, hogy az incidensek során általában a tárolt, kezelt vagy továbbított személyes adatokat sérelem éri, amely jellegét tekintve lehet véletlen vagy jogellenes (szándékos), megsemmisülés (helyreállíthatatlanul törölt), elvesztés (sérül a rendelkezésre állás elve), módosítás (integritás sérülése), jogosulatlan közlés (adatszivárgás) vagy hozzáférés (sérül a bizalmasság elve). Amennyiben az adatvédelmi incidenst figyelmen kívül hagyják vagy nem a megfelelő

intézkedés követi, vagyoni és nem vagyoni károkat okozhat a természetes személyeknek és az intézményeknek, vállalkozásoknak egyaránt, úgymint személyes adataink feletti rendelkezés elvesztését, hozzáférési jogosultságok korlátozását, személyazonosság illegális felhasználását, pénzügyi veszteséget és még számos, személyes adathoz köthető károkozást, jelentős szociális vagy gazdasági hátrányt. A károkozás mértékének csökkentése érdekében az adatvédelmi incidenst, késedelem nélkül, [265] lehetőleg a tudomást szerzéstől számított legkésőbb 72 órán belül a Hatóság (az illetékes felügyeleti hatóság) felé be kell jelenteni. Amennyiben a bejelentés 72 órán belül nem tehető meg, rögzíteni kell a késedelem okát és a részleteit is. Az incidenskezelés során meg kell vizsgálni a technológiai védelmi és szervezési intézkedéseket és azok végrehajtásának eredményeit. Az adatok és a védelem helyreállítása esetfüggő, de tekintettel a személyes adatok érintettségére minden esetben a mindenkor rendelkezésre álló technológiai és elvi módszerek alkalmazásával a legkörültekintőbb módon kell eljárni. Az adatvédelmi incidenseket a jelentőségükre való tekintettel a Hivatal is kiemelten kezeli. Az adatvédelmi incidensek vonatkozásában 2019. évben 276 hatósági eljárásból 37 kérelemre indított és 15 hivatalból indított ügyben, míg 2020. évben 347 hatósági eljárásból 13 kérelemre indított ügyben és 16 hivatalból indított ügyben rögzítettek adatvédelmi incidenst.[266] 2019. évben a nyilvánossá tett határozatok 15%-a, míg a következő évben 9%-a tartalmazott adatvédelmi incidensre vonatkozó megállapítást. Ez az érték 2021. évben tovább csökkent, tehát megállapítottam, hogy csökkenő tendenciát mutat. Ez az érték a bejelentett vagy hivatalból vizsgált esetekre, nyilvános határozatokra vonatkozik. Tehát a bejelentésre került és kivizsgált adatvédelmi incidensek száma csökkent, ugyanakkor a hatósági eljárások száma megnövekedett a 2019-2020. években. A határozatok tekintetében a megállapított adatvédelmi bírság számának aránya 2019-2020. években nem változott (57%), míg 2021-ben csökkent (48%). A bejelentett incidensek száma évről-évre nő (2019-ben 506, míg 2020-ban 781 adatvédelmi incidens bejelentés történt), azonban azon incidensek számát nem növelik azok az esetek, ahol bár megtörtént az informatikai támadás, de adatvesztésre vagy harmadik fél általi hozzáférésre és adatkinyerésre nem került sor, vagy a személyes adatok nem kerültek nyilvánosságra, illetve a nem szándékos adattovábbítás következtében a harmadik félhez került adatokat helyreállíthatatlan módon törölték.[267]

[265] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR), Preambulum (85)-(88)
[266] NAIH 2020. évi beszámolója, adatvédelmi hatósági eljárások, ügyszámra vonatkozó adatok 2020.
[267] NAIH 2020. évi beszámolója, bejelentett adatvédelmi incidensek száma 2018-2020.

3.2.4. ADATVÉDELMI ALAPELVEK TELJESÜLÉSÉNEK VIZSGÁLATA

A nyilvános határozatok tekintetében a vizsgálat során megállapítottam, hogy a megállapítások, a figyelmeztetések, a kötelezések valamint a végzések száma is nőtt az elmúlt években. A nyilvános határozatok statisztikai adatainak vizsgálata alapján, a következő alapelvekre fókuszáltam a 2020. évben: tájékoztatási kötelezettség, hozzáférési jog, adattakarékosság elve, valamint a kamerahasználattal, hangfelvétellel kapcsolatos jogsértések. A vizsgált időszakban a tájékoztatási kötelezettség elmulasztása[268]: 46%, ami az előző évhez képest duplájára nőtt, és 2021-ben már 52%-ot mutatott.

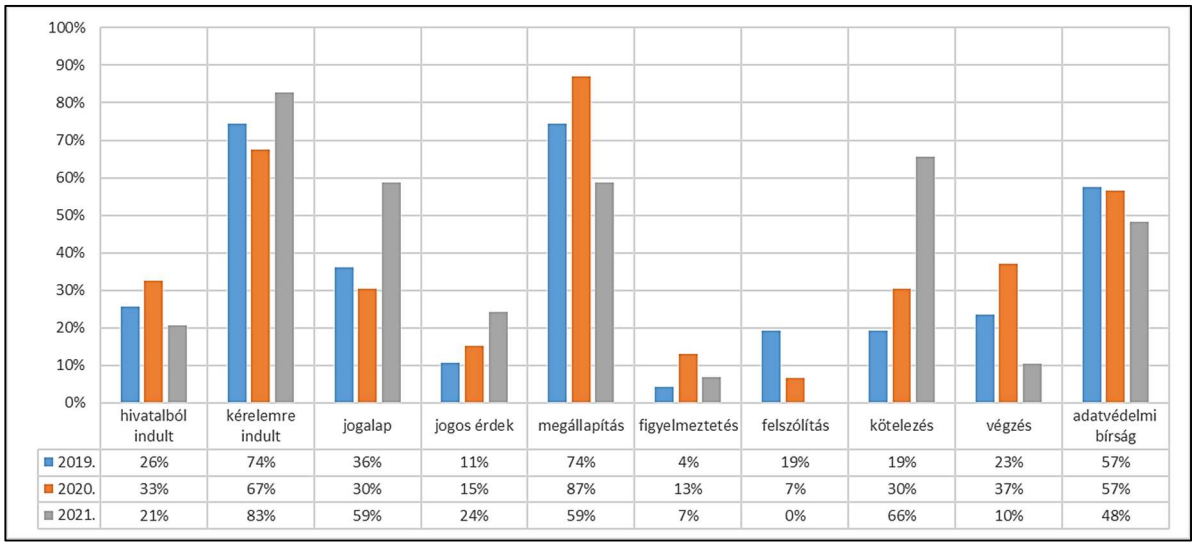
Év / Megnevezés	2019. Határozatok száma összesen		2020. Határozatok száma összesen		2021. Határozatok száma összesen	
Vizsgált nyilvános határozat	**48**		**47**		**29**	
ebből:						
hivatalból indult	12	26%	15	33%	6	21%
kérelemre indult	35	74%	31	67%	24	83%
adatvédelmi bírság	27	57%	26	57%	14	48%
adatbiztonság	3	6%	5	11%	2	7%
adatvédelmi incidens	7	15%	4	9%	1	3%
adatkezelés	4	9%	4	9%	3	10%
közös adatkezelés	1	2%	0	0%	1	3%
adattovábbítás	7	15%	4	9%	8	28%
tájékoztatási kötelezettség	9	19%	21	46%	15	52%
jogi kötelezettség	4	9%	1	2%	2	7%
adattakarékosság	8	17%	7	15%	3	10%
különleges adat	4	9%	4	9%	5	17%
másolatkészítés/másolás	6	13%	4	9%	0	0%
hozzáférési jog	12	26%	15	33%	8	28%
törléshez való jog	9	19%	7	15%	6	21%
átláthatóság	4	9%	5	11%	4	14%
célhoz kötöttség	8	17%	6	13%	5	17%
elszámoltathatóság	2	4%	0	0%	4	14%
pontosság	2	4%	3	7%	1	3%
hangfelvétel/ kamera	8	17%	7	15%	8	28%
közérdekből nyilvános adat	1	2%	5	11%	3	10%
követeléskezelés	4	9%	4	9%	4	14%

4. táblázat, A NAIH által nyilvánossá tett határozatai alapján készített statisztikai adatok, ügyek aránya, 2019-2021., saját adatgyűjtés és vizsgálat alapján

A hozzáférési jog megsértése: 33%, 2021-ben 28%, tehát 30% körüli értéket mutat, az adattakarékosság elvének sértése: 15%, 2021-ben 10%, míg a törléshez való jog megsértése: 15%, 2021-ben 21% volt. A kamerahasználattal, hangfelvétellel kapcsolatos jogsértések: 15%,

[268] „*Az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez.*" (32)
AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)

aminek értéke 2021. évre némiképp emelkedett: 28%-ra nőtt. A célhoz kötöttség elvének sértése: 13%, 2021-ben 17%, míg az átláthatóság megsértése: 11%, 2021-ben 14%-os értéket mutatott.



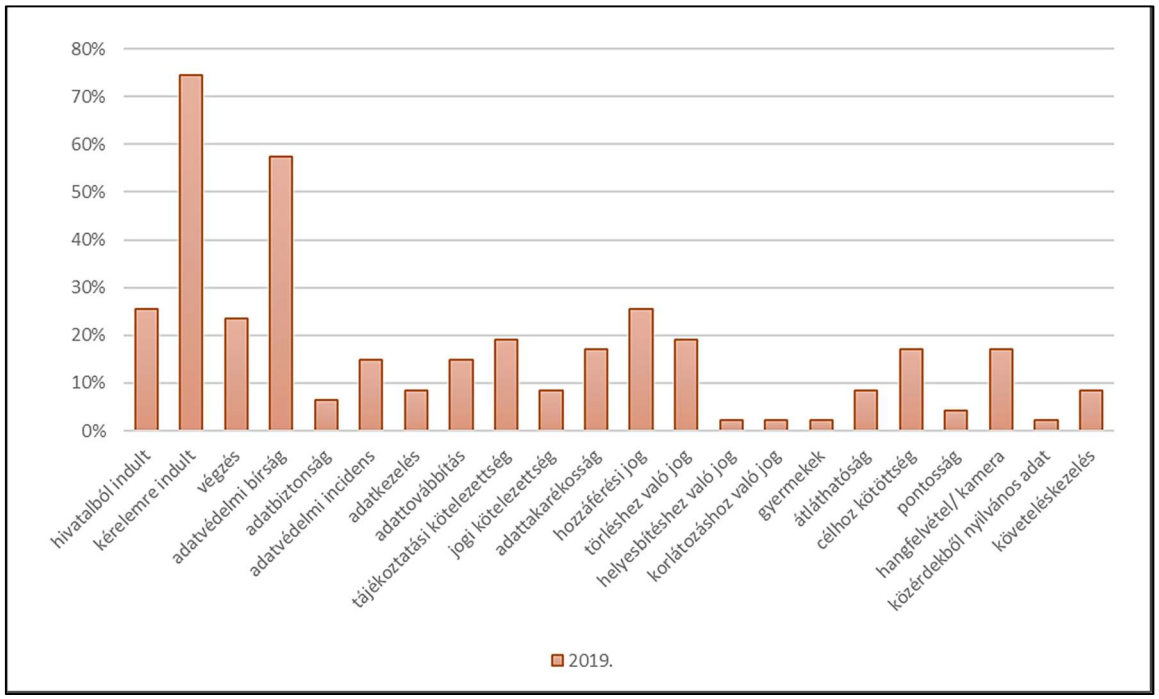
	hivatalból indult	kérelemre indult	jogalap	jogos érdek	megállapítás	figyelmeztetés	felszólítás	kötelezés	végzés	adatvédelmi bírság
2019.	26%	74%	36%	11%	74%	4%	19%	19%	23%	57%
2020.	33%	67%	30%	15%	87%	13%	7%	30%	37%	57%
2021.	21%	83%	59%	24%	59%	7%	0%	66%	10%	48%

1. ábra, NAIH nyilvános határozatok statisztikai adatainak vizsgálata

2019-2021. saját adatgyűjtés, vizsgálat alapján, saját szerkesztés

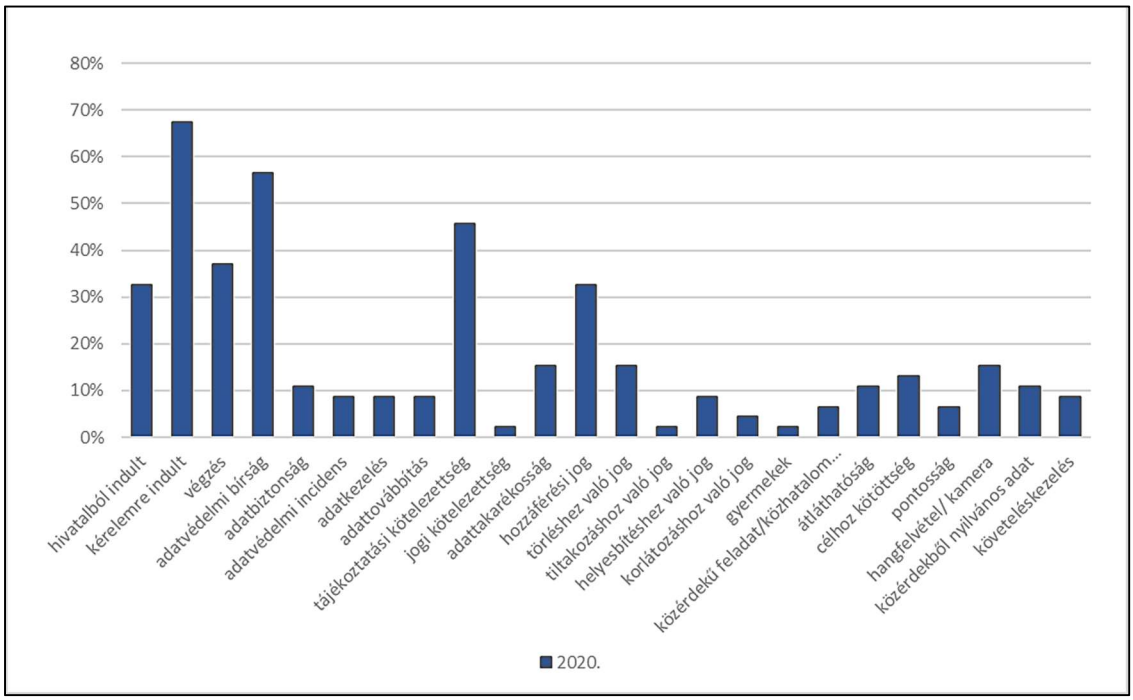
A NAIH által 2019-2021. években nyilvánosságra hozott anonim vagy részben publikus határozatokat megvizsgálva (például: NAIH-3211-14/2021 sz. határozat), következtethető, hogy a Hatóság leginkább megállapítást (különösen általános adatvédelmi rendelet rendelkezéseinek például elszámoltathatóság, adatvédelmi jogsértést, jogszerűség vagy adatkezelés elvének megsértését), az adatvédelmi bírság megfizetésére vonatkozó kötelezést, valamint a kötelezést (például értesítési kötelezettség felvétel törlésének szükségességéről) alkalmazott (1. ábra).

2019. évi statisztikai elemzés alapján (2. ábra) az adatvédelmi jogsértések közül a legtöbb esetben a hozzáférési és törléshez való jogmegsértés, valamint a tájékoztatási kötelezettség elmulasztása fordult elő, de egyik sem érte el a vizsgált esetek 30%-át, míg 2020-ban a tájékoztatási kötelezettség elmulasztása meghaladta a 40%, ami 2021-ban ez már 52% volt. A tájékoztatási kötelezettség elmulasztásának hátterében az adatkezelő és az érintett felek közti kommunikációs probléma is vezethet a kötelezettség elmulasztásához. (3., 4. ábra)



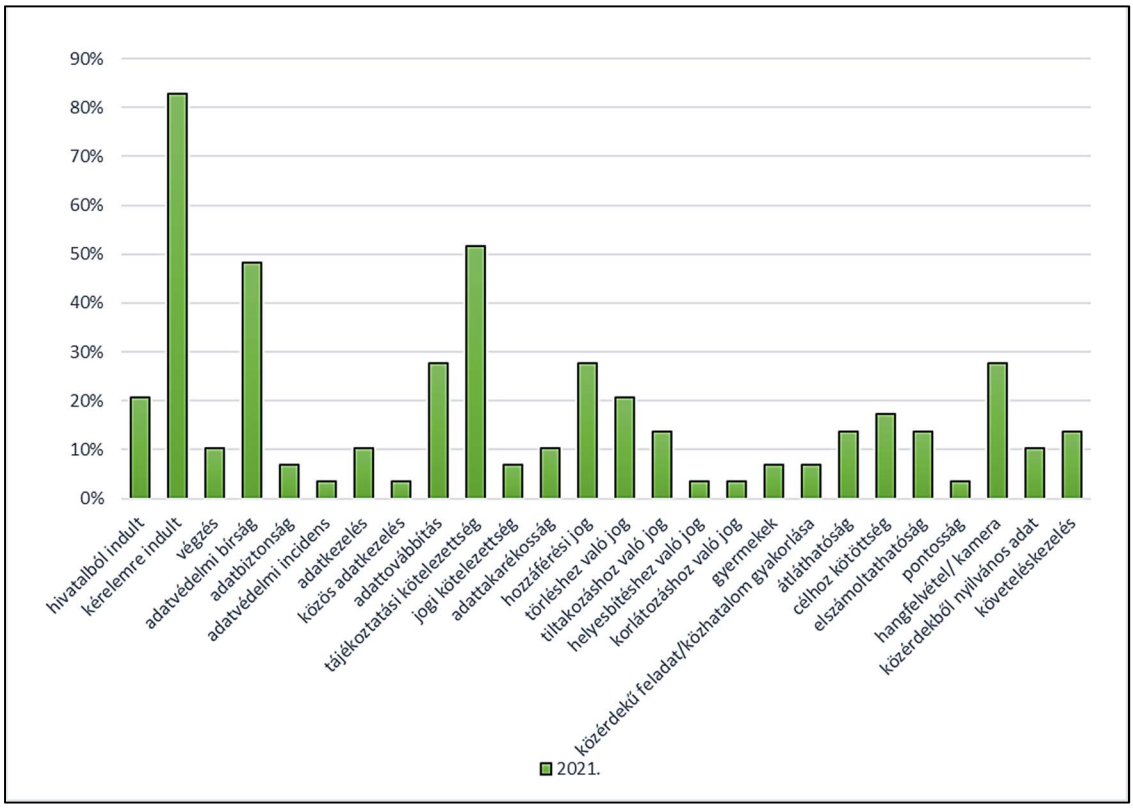
2. ábra, NAIH nyilvános határozatok statisztikai adatainak vizsgálata

2019. saját adatgyűjtés, vizsgálat alapján, saját szerkesztés



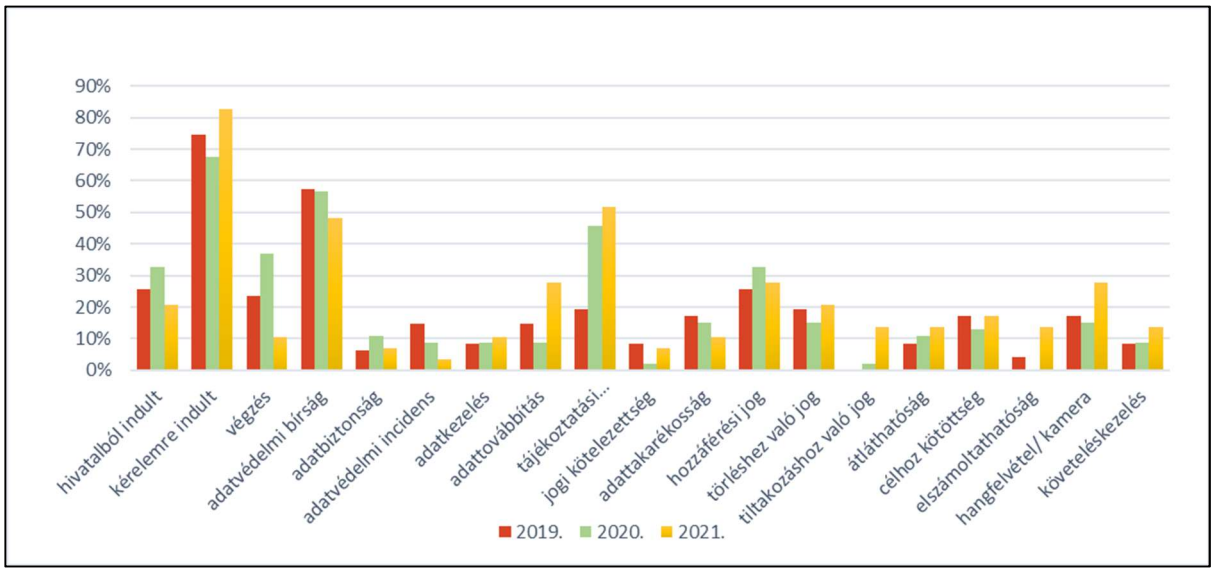
3. ábra, NAIH nyilvános határozatok statisztikai adatainak vizsgálata

2020. saját adatgyűjtés, vizsgálat alapján, saját szerkesztés



4. ábra, NAIH nyilvános határozatok statisztikai adatainak vizsgálata

2021. saját adatgyűjtés, vizsgálat alapján, saját szerkesztés



5. ábra, NAIH nyilvános határozatok statisztikai adatainak vizsgálata

2019-2021. saját adatgyűjtés, vizsgálat alapján, saját szerkesztés

A 2019-2021. évek statisztikai adatait összehasonlítva megállapítható, hogy a tájékoztatási kötelezettség elmulasztása, valamint a hozzáférési jogsértések az adatvédelmi eljárások és

határozatok tekintetében továbbra is jelentős, adatvédelmi incidenshez és bírság megállapításhoz vezető jogsértések, ugyanakkor a nem jogszerű adattovábbítás, illetve hang és kamerafelvétel rögzítése és tárolása egyre növekvő tendenciát mutat. Ez utóbbi jogsértések kiváltó oka lehet a megnövekedett, ellenőrizetlen online kamerahasználat vagy kommunikáció információbiztonsági szabályainak figyelmen kívül hagyása. A rendelkezésre álló adatok alapján összességében megállapítható, hogy a hivatalból vagy kérelemre indult hatósági eljárások tekintetében az adatvédelmi incidens csökkenő tendenciát mutat. (5. ábra) Az ügyek tekintetében a tájékoztatási kötelezettség elmulasztásának vizsgálata szerepelt legtöbbet. A NAIH/2020/4762/9. számú kérelemnek részben helyt adó határozat tárgyú ügyben a Hatóság megállapította, hogy a kérelmezett nem biztosította a kérelmező hozzáférési jogát és nem tett eleget a tájékoztatási kötelezettségének, mivel a GDPR előírásának megfelelően az előírt egy hónapos határidőn belül nem tájékoztatta a kérelmezőt kérésének megfelelően és figyelmeztetésben részesítette. Az adatkezelő a kérelmező bejelentésétől számított egy hónapon belül köteles tájékoztatni kérelme szerinti intézkedésekről[269], az ügye állapotáról, amennyiben a határidő további legfeljebb két hónapos meghosszabbítása indokolt. A Hatóság rögzítette a tájékoztatáshoz fűződő jog jelentőségét, mivel a modern infokommunikációs technológiák lehetőséget nyújtanak a nagy mennyiségű információgyűjtésre, tárolásra, valamint feldolgozásra sok esetben mindez az érintettek tudtán és beleegyezésén kívül teszik. A nagymértékű adatgyűjtés és feldolgozás visszaéléseket, és az érintettek jogai és érdekei figyelmen kívül hagyásával, illetve sérülésével követik el. A tájékoztatás egyik módja az információs monopólium kialakulásának megakadályozása. A tájékoztatás értelmezésével az érintett saját maga dönthet az adatkezelés mértékéről annak függvényében, hogy a tervezett adatkezelés milyen hatást gyakorolhat a magánéletére és egyben egy módja annak, hogy gyakorolhatják információs önrendelkezési jogukat.[270] Az Infotv. és a NAIH állásfoglalásai alapján összegeztem, hogy adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű módon hozzájárul személyes adatainak kezeléséhez, mint például írásbeli, elektronikus úton tett, vagy szóbeli nyilatkozat által tett, illetve önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulás. Hozzájárulásnak minősül különösen, ha az érintett internetes honlap megtekintése közben bejelöl az adatkezelésre vonatkozó adatbeviteli mezőt, négyzetet, tehát a

[269] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR), 12. cikk (3) bekezdése

[270] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: kérelemnek helyt adó határozat, Ügyszám: NAIH/2020/4762/9.

visszajelzés egyértelműen igazolható, továbbá az információs rendszerszolgáltatás igénybevételekor technikai beállítást hajt végre, vagy bármely olyan nyilatkozat vagy arra utaló magatartás, amely az adott hozzájárulással kapcsolatban az érintett hozzájárulását egyértelműen jelzi. Az érintettet az adatgyűjtés időpontjában vagy azt megelőzően kell tájékoztatni az érintettel kapcsolatos adatgyűjtésről. A tájékoztatásnak a következő, legkevesebb tartalommal kell rendelkeznie: az adatkezelő vállalkozás vagy intézmény adatai, az adatkezelő az adatvédelmi tisztviselőjének megnevezése és elérhetősége, az adatkezelés oka és célja, az érintett személyes adatok kategóriái, úgymint például: név, születési név, anyja neve, adóazonosító jele, elérhetőség, munkaügyi adatok, béradatok, az adatkezelés jogalapja, az adatkezelő által tárolt adatok megőrzésének ideje, az adatfeldolgozó vagy harmadik személy megnevezése, amennyiben van ilyen. Továbbá tartalmaznia kell az Európai Unión kívülre való továbbítás szükségességének rögzítése, esetleges indoklását, esetleges hivatkozást az érintett adatainak másolati példányára, tekintettel arra, hogy joga van az adatok egy példányához (az adatokhoz való hozzáférés joga), továbbá a tájékoztatást egyéb adatvédelmi alapvető jogokról, a panaszbenyújtás jogára vonatkozókat (az érintettnek joga van panaszt benyújtani a Hatósághoz), az érintett hozzájárulásának visszavonására vonatkozó jogot; az esetleges automatizált adatkezelésen alapuló döntéshozatal alkalmazását, valamint következményeit. Az időben nyújtott és tartalomban megfelelő, valamint az érintett kérését kielégítő adatkezelői tájékoztatás az adatkezelési átláthatóság, a tisztességes eljárás követelménye szempontjából is jelentős. Az átláthatóság elve megköveteli a személyes adatok kezelésével összefüggő tájékoztatás nyújtását, valamint a tájékoztató könnyen hozzáférhető, közérthető, világos és egyszerű megfogalmazás legyen.[271] Véleményem szerint a tájékoztatás segíti az érintettet a számára biztosított adatvédelmi jogok gyakorlásában, az adatvédelmi ellenőrzést tevékenységét, az esetleges jogorvoslat igénybe vételét, amelyet a Hatóság eljárásai is tükröznek. Az érintettnek számára biztosítani kell az adatvédelmi jogok gyakorlását, mivel a vonatkozó rendelkezések szerint joga van tájékoztatást kérni személyes adatainak kezeléséről, hozzáférést kérni a róla tárolt személyes adatokhoz, adatainak helyesbítését kérni, személyes adatai törlését kérni, tiltakozni különösen a marketingcélokra történő feldolgozás ellen, személyes adatai kezelésének korlátozását kérni, adatainak elektronikus formátumú elküldését kérni, és élni az adathordozhatóság jogával, az automatizált adatkezelésen alapuló döntések,

[271] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR), Preambulum (32), (39), 15. cikk

különös tekintettel a profilozás ellen kifogással vagy panaszbenyújtás jogával élni. Az érintettnek joga van tájékoztatást kérni az adott vállalkozástól, intézménytől milyen típusú, és tartalmú személyes adatokat tárolnak róla. Tehát az érintettnek joga van hozzáférni a személyes adataihoz, azokról másolatot kérni, valamint további, az adataival kapcsolatos információt kérni, különösen a tárolás céljára, okára és idejére, az adatainak forrására vagy az adatkategóriára vonatkozóan. A hozzáférési vagy bármely adatvédelmi jog nem érintheti hátrányosan más természetes személyek jogait, az üzleti titkokat vagy a szellemi tulajdonra, szerzői jogra vonatkoztatható jogokat. A Hatóság által nyilvánosságra hozott anonim adatokat tartalmazó határozataiban, eseteiben rögzítésre került a hozzáférési jog vizsgálatával kapcsolatban hozott döntései közül a NAIH/2020/876/12. számú[272] ügyben a Hatóság a kérelemnek részben helyt adott és megállapította, hogy a kérelmezett a hozzáférési jog alapján nem tájékoztatta a kérelmezőt a róla kezel személyes adatokról, információkról. A kérelmező a meghiúsult automatából történt bérletvásárlás okán tájékoztatást kért arról, hogy az vásárlási kísérlet során milyen személyes adatok kerültek vagy róla készült videófelvétel került rögzítésre. A kérelmezett tájékoztatása nem tartalmazta erre irányuló válaszát, tehát nem tájékoztatta megfelelően a kérelmezőt és a kérelmezett, mint adatkezelő nem nyújtott megfelelő, átlátható tájékoztatást az általa kezelt adatokra vonatkozóan. A kérelmezett megsértette a GDPR 12. cikk (1) bekezdését és a 15. cikket, valamint a kérelmezőt meggátolta hozzáférési jogának gyakorlásában, GDPR alapelvei tekintetében sérült az érintett hozzáférési joga. A Hatóság a GDPR 58. cikk (2) bekezdés c) pontja alapján utasította az adatkezelőt, hogy teljesítse a kérelmező hozzáférésére, tájékoztatásra, adatkezelésre irányuló kérelmét. Az adatvédelmi bírság kiszabása ügyében a Hatóság a GDPR 83. cikk (2)[273] bekezdése és az Infotv. 75/A. §-a alapján[274] megállapította, hogy az adatvédelmi bírság kiszabása szükséges. A nyilvános határozatok vizsgálata során megállapítottam, hogy a Hatóság az esetek közel 50%-

[272] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: kérelemnek részben helyt adó határozat, Ügyszám: NAIH/2020/876/12. (NAIH/2019/8236.)

[273] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR), 83. cikk A közigazgatási bírságok kiszabására vonatkozó általános feltételek

[274] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) 75/A. § „*A Hatóság az általános adatvédelmi rendelet 83. cikk (2)-(6) bekezdésében foglalt hatásköreit az arányosság elvének figyelembevételével gyakorolja, különösen azzal, hogy a személyes adatok kezelésére vonatkozó - jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott - előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt - az általános adatvédelmi rendelet 58. cikkével összhangban - elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik.*”

ban döntött adatvédelmi bírság kiszabásáról. A Hatóság a bírság mértékénél figyelembe vette az érinett szervezet nettó árbevételét és az időszakra vonatkozó gazdasági adatait is.[275]

3.3. ADATVÉDELMI ESETEK VIZSGÁLATA

3.3.1. ADATVÉDELMI INCIDENSEKEK VIZSGÁLATA ÉS INCIDENSKEZELÉS

Ebben a fejezetrészben néhány adatvédelmi incidensben meghozott és általam vizsgált hatósági határozat alapján az adatvédelmi alapelvek és szabályok jelentőségére szeretném felhívni a figyelmet. Adatvédelmi incidens akkor következik be, amikor az információs rendszer sérülékenységét kihasználva az adatvédelmi és az információbiztonsági elvek sérülnek, ezáltal az érintett adatvédelmi jogaira nézve kockázatot jelent.[276]

3.3.1.1. ADATVÉDELMI INCIDENS UTAZÁSI IRODÁNÁL

Az adatvédelmi incidensek közül korábban már említett eset egy utazási iroda által 2019. év végén és 2020. év elején kezelt személyes adatok bizalmas jellegének sérülésével kapcsolatos magas kockázatú adatvédelmi incidens bekövetkezett be. Az iroda által üzemeltetett honlapon keresztül elérhetővé váltak az iroda tevékenységéhez kapcsolódó ügyfelek személyes adatai, többek között az utasok neve, elérhetősége, lakcím adatok, igazolvány és okmányok adatai, valamint a foglalással kapcsolatos adatok, úgymint utazás időpontjai, úti cél, foglalás státusza és száma, szállás adatok és a megkötött szerződés tartalma.[277] A hivatalból indított adatvédelmi hatósági eljárásban rögzített incidensre egy közérdekű bejelentés hívta fel a figyelmet, amit az

[275] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban Ügyszám: NAIH/2020/66/21

[276] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)
Preambulum (49) „*Az érintett adatkezelő jogos érdekének minősül a közhatalmi szervek, számítástechnikai vészhelyzetekre reagáló egység (CERT), hálózatbiztonsági incidenskezelő egységek (CSIRT), elektronikus hírközlési hálózatok üzemeltetői és szolgáltatások nyújtói, valamint biztonságtechnológiai szolgáltatók által végrehajtott olyan mértékű személyes adatkezelés, amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos, vagyis adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képessége az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek által nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben.*”
4. cikk 12. pont „*’adatvédelmi incidens’: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi*;”

[277] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban Ügyszám: NAIH/2020/66/21

interneten kereshető utazáshoz köthető személyes adatok indokoltak. A Hatóság a bejelentést követően ellenőrizte a bejelentett információk valódiságát és megállapította, hogy az internetes keresőrendszer segítségével elérhetővé váltak az utazási iroda ügyféleinek adatai, a személyes adatok jogosultságellenőrzés vagy egyéb informatikai biztonsági beállítás nélkül az utazási iroda weboldalán elérhetőek és az ott talált adatbázisból lekérhetők. A tartalmat az internetes keresőrendszer is letárolta, azokat kulcsszavas kereséssel kereshetővé tette (beindexelte). A keresőrendszer előnye, hogy a webes robotok több százmilliárd weboldalról gyűjtenek információt, majd rendszerezik őket a keresési indexben, ezáltal gyorsabb elérhetőséget és megjelenítést tesznek lehetővé. A keresőrobotok meglátogatják a weboldal oldaltérképeit, majd az ott fellelhető linkek segítségével további oldalakat fedeznek fel. A Google Keresés indexe weboldalak százmilliárdjait tartalmazza, mérete valószínűleg meghaladja a 100 000 000 gigabájtot. A keresés indexe olyan, mint egy tárgymutató, mivel külön bejegyzés tartozik minden beindexelt weboldal, minden egyes szavához. Az indexelés alapötlete a könyv tárgymutatóján és a tartalomjegyzéken alapul, aminek segítségével megtalálható az adott könyvben keresett szó vagy téma. A könyv katalógus alapján kereshető, akár egy könyvtárban. A keresőrendszer lényegében egy virtuális könyvtár, aminek polcain weboldalak és azok mögött információk sokasága rejlik. Az információkeresés segítsége az úgynevezett kereső algoritmus, a könyvtáros, aki minden meglévő információt megtalál a polcon, vagy a hiányzókat felkutatja. A keresőrendszer eredménye a világot behálózó internet segítségével, a weboldalak információiból összegyűjtött világméretű adatbank. Egy-egy hibás vagy védett tartalom eltávolítása éppen ezért meglehetősen bonyolult feladat, talán lehetetlen, hiszen nem tudjuk, hogy az adott információt esetleg nem mentette le egy adott kliens számítógép. Éppen ezért az interneten egyszer már megjelent tartalmat, többé már nem lehet teljes mértékkel védetté tenni. A keresőrendszerből kérelem alapján el lehet ugyan távolítani a nem publikus webcímet, de annak tartalmának törlése a világ egy másik pontján lévő számítógépről, vagy egyéb adattárolóról már meglehetősen nehéz művelet. Továbbá az illetéktelen személyhez került személyes adatok nem megengedett felhasználása már kevésbé kontrollálható. A törlési művelet bonyolultsága miatt is kritikusnak tekinthető az adatvédelmi incidens, a személyes adatokat tartalmazó adatbázis interneten való kereshetősége. Az incidens vizsgálata során megállapították, hogy az utazási iroda webes felülete nemcsak az adatletöltést, de a fájlfeltöltést és az adatmódosítást is megengedte, így lehetőség volt nemcsak az útlevélfotó képét, de bármilyen típusú fájlt feltölteni. A Hatóság által talált 375 rekord nagy része valós személyek adatát tartalmazta. Az utazásokhoz kapcsolódó szerződések, az összes szerződő utas személyes

adatát tartalmazta. A Hatóság az ellenőrzés során online figyelemmel tudta követni az adatbázis frissítését, új szerződések és személyes adatok feltöltését és azok nyilvános hozzáférését. A Hatóság a végzéssel nyilatkozattételre és iratszolgáltatásra szólította fel az adatkezelőt, aki nyilatkozatában kiemelte, hogy a nyilvánossá vált személyes adatokat tartalmazó adatbázist teszt jelleggel üzemeltették és az adatfeldolgozó látta el a weboldal informatikai szolgáltatásával kapcsolatos feladatokat. Az adatkezelő az adatvédelmi incidensről a Hatóság végzésének kapcsán szerzett tudomást, az adatfeldolgozó megszűntette az adatbázis nyilvános hozzáférését és különböző információbiztonsági beállítást alkalmazott (tűzfalszabály, többszintű azonosítás és hozzáférési jogosultság ellenőrzés, jelszóerősség vizsgálat, biztonsági adatmentés, eseménynaplózás) és nagymértékben csökkentette az ügyféladatbázis és a weboldal sebezhetőségét. Az adatkezelő együttműködött a Hatósággal, határidőben eleget tett a felszólításnak, és a végzésben foglaltak szerint járt el. Az adatkezelő által nyilvántartott, de az incidens részleges időtartalmáról rendelkező eseménynapló szerint összesen két IP címről történt illegális, jogosulatlan hozzáférés az adatbázishoz. Az adatkezelő és az adatfeldolgozó korábban adatfeldolgozói megállapodást kötött, amely rögzítette az adatfeldolgozó az adatok biztonságos feldolgozására és adatvédelemre vonatkozó feladatát és kötelezettségeit, valamint a biztonságos adatfeldolgozás garantálását és a felelősségvállalást. A Hatóság az adatvédelmi hatósági eljárásba az adatfeldolgozót is bevonta. A további hatósági ellenőrzés során az adatkezelő címén már nem vették át a hatósági kézbesítéseket, mert az adatkezelő cége felszámolás alatt állt. Az utazási iroda által használt adatbáziskezelő nem megfelelő biztonsági beállításából eredő sérülékenysége által 309 utazási szerződéshez, 781 érintett közel 2500 személyes adatához lehetett hozzáférni. A Hatóság megállapította, hogy az adatkezelő megsértette a GDPR 25., 32., 34. cikkét, az adatfeldolgozó a GDPR 32. cikkét és a nem megfelelő információbiztonsági, technikai beállítások miatt a személyes adatok nyilvánossá válása következtében sérültek az érintettek adatvédelmi jogai, a Hatóság mind az adatkezelőt és az adatfeldolgozót adatvédelmi bírság megfizetésére kötelezte. A bírság megállapításánál enyhítő körülményként figyelembe vették, hogy érintetteket igazolt kár nem érte, a jogsértés nem volt szándékos és a tudomásszerzést követően intézkedtek a feltárt biztonsági rés megszüntetéséről, amelynek következtében a sérülékenység megszűnt. Véleményem szerint az incidenskezelés helyett célszerűbb az információbiztonsági preventív folyamatokat alkalmazni és a megelőző intézkedésekre nagyobb hangsúlyt fektetni. Az esetvizsgálatok alapján megállapítottam, hogy az adatbáziskezelők adatvédelmi és információbiztonsági folyamatait és beállításait a meghatározott elvek szerint lehet kialakítani, amelyeket a NAIH állásfoglalások

is megerősítenek, így különösen legyen elkülönítve az alkalmazás és az adatbázisszerver, a teszt és az éles rendszer egymástól elkülönített szerveren kerüljön kialakítása, a szerver tűzfalbeállítások alkalmazása elengedhetetlen, a hozzáférésellenőrzési előírások szerint szükséges a szerver, az alkalmazásszerver és az adatbázisszerver jogosultságkezelésének beállítása és rendszeres ellenőrzése (napló állományok), jogosultság szintek meghatározása és alkalmazása, valamint erős jelszó policy beállítása, admin és adatgazdai feladatkörök elválasztása, továbbá a biztonsági adatmentés szabályainak kialakítása elengedhetetlen, úgymint rendszeres adatmentés és visszatöltés, valamint az adatbázis visszatöltésének rendszeres ellenőrzése a teszt rendszerben egyaránt. Az adatbázis és alkalmazás informatikai keretrendszerek biztonsági frissítéseinek alkalmazása a teszt rendszerekben, majd eredményes tesztrendszer frissítés után szükséges az éles rendszerek biztonsági frissítése is. Az adatbázis és alkalmazás fejlesztését először a teszt rendszerekben kell kipróbálni, illetve megvalósítani, majd a hibakezelés és eredményes, hibamentes tesztrendszerek futtatása után alkalmazható az éles rendszerekben is. Minden adatbázisműveletet, hozzáférést és rendszerfrissítést naplózása szükséges. A fenti elveket a 2016-2022. időszakban betöltött alkalmazásadminisztrátori feladatköröm ellátása során gyakorlatban is alkalmaztuk, amely során több alkalommal bebizonyosodott, hogy az alapelvek és arra épülő szabályok betartása elengedhetetlen, mivel elsődlegesen az adatvédelmi incidensek bekövetkezések (például adatvesztés, jogosultsággal való visszaélés, adatszivárgás) számát csökkenti. Míg egy hibás informatikai eszköz a rendelkezésre álló pénzügyi keret mértéke szerint pótolható, vagy a konfiguráció, programrészlet javítható, addig az elveszett adat, másolatpéldány nélküli adathalmaz vagy az illetéktelen, rosszindulatú felhasználás nehezen orvosolható.

3.3.1.2. ADATVÉDELMI INCIDENS ADATVESZTÉS ÁLTAL

A fejezetben vizsgált 2019. évben a Budapesti Rendőr-főkapitányság által bejelentett adatvédelmi incidenssel kapcsolatban a Hatóság megállapította, hogy a személyes adatokat tartalmazó pendrive elvesztése során az adatkezelő nem tett eleget a tudomásszerzéstől számított 72 órán belüli incidensbejelentési kötelezettségének, és ezáltal megsértette a GDPR 33. cikk (1) bekezdését. Az ügy kivizsgálása során a Hatóság rögzítette a tényeket, miszerint a Budapesti Rendőr-főkapitányság alkalmazottja feladata ellátásának következtében a 4GB méretű tárhellyel rendelkező adathordozót elvesztette, rajta az intézmény személyi állományának 1733 érintett személyes adatait (születési név, születési idő, anyja neve, TAJ szám, beosztás, munkakör) tartalmazó titkosítás nélküli adatállományai. A felelős személy, aki az adathordozót elhagyta magáncélra használt adathordozón tárolta az Intézmény

alkalmazottainak személyes adatait, a használt adathordozó és az adatfájlok biztonsági beállításokat nem tartalmaztak, úgymint hozzáféréshez szükséges felhasználónév és jelszó, fájltitkosítás, valamint megszegte az Intézmény Informatikai Biztonsági Szabályzatában foglalt előírásokat, továbbá gondatlanságának következtében a személyes adatokat tartalmazó adatfájlok elvesztek, és az adatok elvesztésének tényét rögzítő részletes jelentést késedelmesen adta le az Intézménynél. Az Intézmény a felelősségét megállapította és fegyelmi eljárást rendelt el. [278] Az elveszett adatfájlokat illetően az adatok nem kerültek nyilvánosságra, ezért valószínű, hogy az adatok megsemmisültek. Az Intézmény a további, hasonló incidensek elkerülése és az információbiztonsági kockázatok csökkentése végett belső ellenőrzést folytatott le, és szabályozta a személyes adatokat tartalmazó adathordozók használatát, többek között azok nyilvántartását és kezelését, átadás-átvételét, megsemmisítését. Kiemelhető pozitívum, hogy az Intézmény a munkavállalók információbiztonsági és adatvédelmi tudatosítását elősegítve felhívta az adatvédelemmel kapcsolatos előírásokra, valamint azok teljes mértékű betartására a figyelmet. A Hatóság az incidensbejelentési kötelezettség határidejének elmulasztása miatt az Intézményt adatvédelmi bírság megfizetésére kötelezte.[279] A fentekben részletezett adatvesztéssel járó adatvédelmi incidens érdekében megtehető intézkedések lehetnek, különösen az informatikai és információbiztonsági szabályok áttekintése és szükségnek megfelelő módosítása, az intézményi és szervezeti egység szintű informatikai, információbiztonsági és adatvédelmi oktatások, tréningek tartása, munkavállalók információbiztonsági tudatos viselkedésének erősítése, az informatikai, technikai biztonsági konfigurációk, alkalmazott titkosítási módszerek áttekintése és esetleges módosítása,[280] az adatvédelmi és információbiztonsági előírások ellenőrzése, az ellenőrzések során megállapított eltérések szerint meghatározott intézkedései tervek megvalósítása és hatékonyságának ellenőrzése, az adatvédelmi hatásvizsgálat lefolytatása, valamint információbiztonsági

[278] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban Ügyszám: NAIH/2019/2471/6

[279] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)
33. cikk Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak
(1) „*Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.*”

[280] Nemzeti Adatvédelmi és Információszabadság Hatóság, állásfoglalás ügyszáma: NAIH/2018/1132/2/K
29. Cikk Szerinti Adatvédelmi Munkacsoport, 0829/14/HUWP 216, 05/2014. számú vélemény az anonimizálási technikákról, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hu.pdf, letöltés: 2021. április 23.

kockázatelemzés és –kezelés végrehajtása. Véleményem szerint az adatvédelmi hatásvizsgálat lefolytatásával, az információbiztonsági kockázatelemzéssel és –kezeléssel, valamint a vizsgálat során kapott eredményekkel, kockázat mértékének meghatározásával könnyebben ellenőrizhető az adott információs rendszer hatékonysága. A vizsgálatokat érdemes az intézkedések megvalósítása előtt és után is elvégezni, így nemcsak a beavatkozáshoz szükséges tényezőket, az információs rendszer gyenge pontjai kimutathatók, de a hatékonyság is mérhetőbb. Az információbiztonsági kockázatelemzés során az emberi tényezőket is figyelembe kell venni.

3.3.2. JOGALAP, CÉLHOZ KÖTÖTTSÉG ÉS ADATTAKARÉKOSSÁG ELVÉNEK ÉRVÉNYESÜLÉSE

Tekintettel arra, hogy az érintettnek jogában áll megerősítést és tájékoztatást kapni a személyével kapcsolatos kezelt adatokról, valamint tájékoztatni kell a személyes adatkezeléssel összefüggő kockázatokról, szabályokról, garanciákról és jogokról, az adatkezelés konkrét céljáról, amelyet egyértelmű módon kell megfogalmazni. Úgy vélem (és az értekezésben közzétett incidens statisztikai adatok is alátámasztják) továbbá, hogy a nagyobb adatbázisokat kezelő szervezetek, úgymint például egyetemek, kormányzati intézmények, valamint legalább 250 munkavállalót foglalkoztató vállalkozások tekintetében a kezelt személyes és üzleti adatokra, valamint azokkal összefüggő, ügyfélkörhöz tartozó adatokra vonatkozóan az információbiztonsági kockázatkezelés, de legalább az Infotv szerinti hatásvizsgálat elvégzése, kiértékelése és vonatkozó intézkedések végrehajtása, eredményességének vizsgálata elengedhetetlen. A személyes adatokat úgy kell gyűjteni és előkészíteni, hogy azok a kezelésük céljára alkalmas és releváns legyen, az adatok körét a meghatározott célhoz szükséges minimumra kell korlátozni. Biztosítani kell, a személyes adatok lehető legrövidebb időtartamú tárolását, és ennek meghatározására az adatkezelő köteles törlési vagy rendszeres felülvizsgálati határidőket megállapítani. A célhoz kötöttség elve mellett esetlegesen megjelenik az adattakarékosság elve is, amely az adatvédelmi elvek technikai intézkedéseire utal (álnevesítés, anonimizálás).[281] A NAIH/2020/2758/4. számú ügyben a GDPR elvek érvényesülését a

[281] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR), Elvek 5. cikk A személyes adatok kezelésére vonatkozó elvek (1) b) „*gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség”)*”

Hatóság hivatalból indult hatósági eljárás keretében vizsgálta. A vizsgálat során megállapították, hogy a jogelőd cég megsértette a GDPR 6. cikk (1) bekezdés, adatkezelés megfelelő jogalapjával 12. cikk (1) bekezdését, 13. cikkét, és az 5. cikk (1) bekezdés a) pontjával összefüggő rendelkezéseket, valamint 5. cikk (1) bekezdés b) és c) pontja szerinti célhoz kötöttség és adattakarékosság alapelvét. A hatósági ellenőrzés, valamint az azt követő adatvédelmi hatósági eljárás alapját a bejelentő általi tájékoztatás adta, miszerint a cég egyik ügyfélszolgálati irodájában hangfelvétel készül az ügyintézés során, de az érintettek arról nem kapnak (megfelelő) tájékoztatást. A tényfeltárás következtében megállapították, hogy a jogelőd cég az ügyfélszolgálati irodáiban hangfelvételre alkalmas berendezéseket üzemeltetett, és azokkal hangfelvételeket készített. A cég a GDPR 6. cikk (1) bekezdés f) pontjára hivatkozva nyilatkozta, hogy a hangrögzítés jogos érdek, valamint az érdekmérlegelési teszt alapján történt, valamint hatásvizsgálatot is készített az adatkezeléssel járó kockázatok felmérése érdekében. A hangrögzítésről a sorszámhúzó rendszeren keresztül tájékoztatta az ügyfeleket, ami a menü betűméretéhez képest fele akkorával valósították meg.[282] A Hatóság megállapította, hogy a jogos érdek ebben az esetben nem bizonyítható, nem találhatóak meg azok az érvek, amelyek az ügyfélélményt, az ügyfelek számára kedvező megoldást hangsúlyozzák, csak a cég gazdasági érdeke, úgymint a gyorsabb és egyszerűbb ügyintézés igazolható. A Hatóság nem tartotta megfelelőnek az érintettek jogainak biztosítása érdekében beépített garanciát sem, mivel nem minősül garanciális elemnek a hangfelvételek öt évig tartó megőrzése, mivel az 2003. évi C. törvény az elektronikus hírközlésről 143.§ (2) bekezdése egy évet határoz meg, valamint összeegyeztethetetlen azzal, ha a cég a hangrögzítést a szerződéskötésre használja. A

---

25. cikk Beépített és alapértelmezett adatvédelem (1) „*Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.*"

[282] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: Határozat hivatalból indult hatósági eljárásban, Ügyszám: NAIH/2020/2758/4.

„*A GDPR 6. cikk (1) bekezdés f) pontja szerinti jogos érdek jogalapra való hivatkozás akkor helytálló, ha az adatkezelés az adatkezelő vagy – az adatkezelő és az érintett személyétől eltérő – harmadik személy érdekében áll, így az érdekmérlegelésben a mérleg egyik oldalán az adatkezelő vagy harmadik személy jogos érdekét, a másik oldalán pedig az érintett(ek) ellenérdekeit kell megjeleníteni, és az ellentétes érdekek egymással szembeállítását követően megállapítani, hogy az érintett jogainak korlátozása arányban áll-e az adatkezelő vagy harmadik személy – e korlátozás által – érvényesülő jogos érdekével.*"

„*Az érdekmérlegelés lényege éppen az, hogy az adatkezelő felismerje a saját érdekeit, felismerje az érintettek ezzel szemben álló érdekeit, és adott esetben arra a konklúzióra jusson, hogy bár az érintettek oldalán felmerülnek olyan szempontok, alapjogok, személyiségi jogok, amelyek akár a hangrögzítés korlátait jelenthetnék, azonban az adatkezelő oldalán felmerülő érdekek erősebbek, jelentősebbek, ezért az érintetti jogok korlátozása szükséges és arányos*."

Hatóság megállapította, hogy a szerződéskötésre használt hangfelvétel-készítés a cég által hivatkozott érintettek érdekeinek érvényesülése érdekében nem szükséges Az érdekmérlegelési tesztben lévő adatkezelési célok és érdekek lényegesen eltérőek. A Hatóság megállapította továbbá, hogy a cég által hivatkozott jogalap, a GDPR 6. cikk (1) bekezdés f) pontjában előírt feltételek ebben az esetben nem állnak fenn, tehát a cég a vizsgált időszakban megfelelő jogalap nélkül készített hangfelvételt a személyes ügyfélszolgálatokon zajló ügyintézésről. A cég általi adatkezelői tevékenység lényegét tekintve nem cél nélküli, de a felsorolt célok álltalános megfogalmazása nem egyértelmű, másrészt nem adatkezelési cél, hanem adatkezelési jogalap. Továbbá nem jogszerű a hangfelvételek rögzítése csupán érdeklődő ügyfelek esetében, valamint a hangfelvétel-készítés tevékenység nem felelt meg a GDPR 5. cikk (1) bekezdés b) pontja szerinti célhoz kötöttség elvének (meghatározottság és egyértelműség hiánya). Mivel a cég az összes személyes ügyintézés teljes folyamatáról hangfelvételt készített, független attól, hogy csak érdeklődés jellegű vagy szerződéskötéssel járt, ezáltal a Hatóság megállapítása szerint nem felelt meg a GDPR 5. cikk (1) bekezdés c) pontja szerinti adattakarékosság elvének. A hangrögzítés csak úgy lehetséges, ha az ügyfelet megfelelő módon tájékoztatták a hangrögzítés lehetőségéről és az ügyfélszolgálat csak abban az esetben indítja el a felvételt, ha ehhez az ügyfél egyértelmű módon beleegyezését adta. Amennyiben a hozzájárulás nem történik meg, úgy a hangfelvételt sem lehet elindítani. A tájékoztatást érthető és egyértelmű módon kell megtenni, és az ügyfélnek lehetőséget kell nyújtani a beleegyezésre vagy a tiltakozásra. A tájékoztatás során figyelembe kellett volna venni a GDPR 13. cikk (1) bekezdés c) és d) pontjában, valamint a (2) bekezdés a) pontjában foglalt előírásokat, amelyet a cég szintén elmulasztott.

A Hatóság a NAIH/2020/2729/15 számú ügyben, kérelemre indított adatvédelmi hatósági eljárásban vizsgálta a munkahelyi kamerarendszer alkalmazását, és ezzel kapcsolatos GDPR elvek teljesülését. Az ügyben érintett cég telephelyén vagyonvédelmi céllal kamerarendszert üzemeltek be, amely nemcsak személy- és vagyonvédelmi funkciót látott el, hanem a munkavállalók munkavégzésének, valamint pihenő idejének megfigyelésére és ellenőrzésére is felhasználnak. A kérelmező hívta fel a Hatóság figyelmét arra, hogy a munkavállalók nem kaptak megfelelő tájékoztatást a kamerás megfigyelés céljáról és jogalapjáról, a kamera elhelyezésére és céljára vonatkozó figyelmeztető jelzések sem kerültek kihelyezésre. A kérelmező a Hatóságnak benyújtott kérelmében kérte a hatósági eljárás lefolytatását és az esetleges jogsértő magatartás megállapítását. A munkavállalók a cég által üzemeltetett kamerarendszer személy- és vagyonvédelmi célzatú működéséről a tájékoztatót a cég belső

internet hálózatán elérhették és az újonnan belépő munkavállalókat tájékoztatták a kamerarendszer funkciójáról.[283] A Hatóság az eljárás során a cégtől kapott adatok és információk, valamint szakmai vizsgálat eredménye alapján döntésében rögzítette, hogy a GDPR 4. cikk 1. pontjában foglalt fogalommeghatározás és a 4. cikk 2. pontja szerint egy ember arca, képmása személyes adatnak, a képfelvétel készítése, valamint az adatokon elvégzett bármely művelet pedig adatkezelésnek minősül, „*a kamerák látószögei úgy kerültek kialakításra, hogy azok a megfigyelt helyiségek terén és az ott található vagyontárgyakon kívül a telephelyen tartózkodó munkavállalókat is figyelnek*", ezért a munkajogi rendelkezése a mérvadók, így különösen az Mt. 42. § (2) bekezdés a) pontja, Mt. 52. § (1) bekezdés b) és c) pontjai és az Mt. 11/A. § (1) bekezdés. A vizsgálat során a Hatóság megállapította, hogy a kamerák úgy vannak elhelyezve, hogy azok legfőképp a vagyonvédelem célját szolgálja, ugyanakkor alkalmas a munkavállalók munkájának intenzivitását is figyelni, munkájukat nyomon követni és alkalmas az adminisztrációs célú munkaállomásról felvételt készíteni. A Hatóság álláspontja szerint ez utóbbi tevékenység indokolatlannak, tehát az adott helyiség ezen részének kamerával való megfigyelése sem a vagyonvédelme, sem pedig a személyvédelme céljából nem indokolt, mivel az adminisztratív munka testi épségre nem jelent veszélyt, vagy testi épséget veszélyeztető jelentősebb kockázati értéke nincs. Tehát az elhelyezett kamerák helyzetüknél fogva alkalmasak a munkavállalók indokolatlan megfigyelésére, ami sérti a GDPR 5. cikk (1) bekezdés b) pontjában rögzített célhoz kötöttség elvét, valamint a szélesebb látókörű kamerabeállítás sérti a GDPR adattakarékosság elvét (5. cikk (1) bekezdés c) pont). A hang, kép vagy videófelvételre alkalmas eszközök üzembe helyezése és használata során

[283] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: Határozat hivatalból indult hatósági eljárásban, Ügyszám: NAIH/2020/2729/15
„*A kamerás megfigyelés céljának Kérelmezett az épületek biztonságának és a vagyoni javak védelmét, továbbá személyvédelmi célokat jelölte meg a fenti, részletes adatvédelmi szabályzatban. A megfigyelés jogalapjaként Kérelmezett jogos érdeke került megjelölésre. Az adatkezelő jogos érdekén alapuló adatkezeléshez szükséges érdekmérlegelési tesztet a szabályzat külön tartalmazza. A szabályzat 3.2. pontja szerint nem telepíthető kamera olyan helyiségekben, illetve olyan látószögben, amely az alkalmazottak munkaközi idejének eltöltése céljából lett kijelölve, továbbá tilos kamerát elhelyezni öltözőben, illemhelyiségben, zuhanyzóban és minden olyan helyen, ahol a képi megfigyelés az emberi méltóság sérelmével járna*."
„*Kérelmezett nyilatkozata szerint a […] telephelyen üzemelő kamerák nem a munkahelyi jelenlét vagy a munkavégzés intenzitásának megfigyelésére irányulnak, hanem vagyonvédelmi célból telepítette azokat. Megfigyelésre nem kerül sor olyan helyiségekben, amelyek az alkalmazottak pihenésére szolgálnak. Kérelmezett megküldte a telephelyen elhelyezett kamerák listáját, továbbá a kamerák látószögét bemutató pillanatfelvételeket. A kamerák hangot nem rögzítenek, a képfelvételeket legfeljebb 30 napig tárolja a rendszer*."
„*Az Mt. 42. § (2) bekezdés a) pontja értelmében a munkaszerződés alapján a munkavállaló köteles a munkáltató irányítása szerint munkát végezni. Ezzel összhangban az Mt. 52. § (1) bekezdés b) és c) pontjai a munkavállaló alapvető kötelességeként határozták meg azt, hogy a munkavállaló köteles munkaideje alatt a munkáltató rendelkezésére állni és munkáját az általában elvárható szakértelemmel és gondossággal, a munkájára vonatkozó szabályok, előírások, utasítások és szokások szerint végezni. E törvényi kötelezettségek megtartása végett az Mt. 11/A. § (1) bekezdése lehetőséget biztosít arra, hogy a munkáltató a munkavállalót a munkaviszonnyal összefüggő magatartása körében ellenőrizze. Ez a jogosultság szükségszerűen együtt jár személyes adatok kezelésével*."

törekedni kell arra, hogy a GDPR, valamint az információbiztonsági alapelveknek megfelelő legyen és egyúttal az előírásokat betartsák. Az előzőekben részletezett adatvédelmi hatósági eljárásokat is figyelembe véve megállapítottam, amely a Hatóság határozatában foglalt megállapítással alátámasztható, hogy sok esetben a GDPR alapelvek csak részben, vagy egyáltalán nem teljesülnek, ezért az néhány GDPR alapelv különösen jelentős, például a jogalap, a célhoz kötöttség vagy az adattakarékosság. A jogalap tekintetében a munkáltató jogos érdekén alapuló adatkezelés alkalmazása indokolt a munkajogi szabályok, illetve személy- és vagyonvédelem teljesítéséhez. A célhoz kötöttség szempontjából lényeges a kamerarendszer üzemeltetés célja, tehát a személy- és vagyonvédelem, de a megfigyelés csak az emberi élet, testi épség, személyi szabadság, illetve vagyonvédelem érdekében alkalmazható. Másrészt a hangfelvétel rögzítése például a szerződéskötés vagy a hibaelhárítás céljából történik, de az érintettet előzetesen, részletesen, és érthetően tájékoztatták a hangrögzítés céljáról, az adattárolás időszakáról és az érintett egyértelműn módon nyilatkozott a hangrögzítés elfogadásáról, ellenkező esetben a hangrögzítés csak személy- illetve vagyonvédelmi célzattal lehetséges. Az adattakarékosság tekintetében, amennyiben kamerarendszert alkalmaznak a kamerákat úgy kell felszerelni, hogy kizárólag a védendő területet, vagy vagyont rögzíthesse, mást nem. A belépő munkavállalók esetében a tájékoztatási kötelezettség megelőző, részletes, és egyértelmű legyen, a megfigyelt terület esetében figyelemfelkeltő, messziről is jól látható jelzést kell elhelyezni. Mindezen elvek és szabályok betartása véleményem szerint sokszor csak közvetett módon csökkentik az incidensek számát, mégis elengedhetetlen, a *szükséges* voltának bizonyítása nehézkes, például a kamerával megfigyelt terület figyelemfelhívó táblái illegális tevékenység csökkentő tényező lehet.

3.4. AZ ADATVÉDELEM TECHNOLÓGIAI VONATKOZÁSAI

Az Ipar 4.0 technológiai fejlődése és az igazodó nemzetközi rendelkezések új kihívások elé állították a személyes adatok védelmét, így a rendelkezéseknek megfelelni akaró szervezeteket is. Az utóbbi egy évtizedben a személyes adatok nemcsak papír alapú, de elektronikus gyűjtése, kezelése és feldolgozása, valamint szükségszerű továbbítása nagymértékben megnőtt, amely további technológiai és szabályozás tekintetű vonatkozásokat jelent a szervezetek életében. A minimális mértékű személyes adatok akár ideiglenes tárolása elengedhetetlen a szervezetek számára, tevékenységük folytatásához a GDPR szabályozási támogatást nyújt. Olyan technológiák tervezését, kivitelezését és alkalmazását kell megvalósítani, amely eleget tesz a GDPR és az Infotv. adatvédelmi előírásainak és egyben elősegíti a személyes adatok Unión

belüli biztonságos szabad áramlását is. A személyes adatok, így az adatok alapján egyértelműen beazonosítható természetes személyek nyilvánvalóan összefüggésbe hozhatók az általuk használt elektronikus eszközökkel, alkalmazások, az IT eszközök és protokollok által összegyűjtött és rendelkezésre bocsátott online azonosítókkal, mint például az IP-címekkel, eszköz azonosítóval (MAC) és egyéb elektronikus azonosítókkal, vagy rádiófrekvenciás azonosító címkékkel. Az ily módon származó adathalmazok tartalmát matematikai statisztikai módszerek alkalmazásával felhasználhatók a természetes személy profiljának, viselkedésének létrehozására, így az adott személy azonosítására. Az intézmények általában törekednie kell arra, hogy a profilozásra irányuló tevékenységre felhívják a munkavállalók figyelmét, ezáltal a felhasználók biztonságtudatosságát erősítsék. Tekintettel arra, hogy az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli (papír alapú vagy elektronikus), illetve szóbeli nyilatkozattal önkéntes, egyértelmű, tájékoztatáson alapuló hozzájárulását adja a személyt érintő személyes adatok kezeléséhez, ezért célszerű erősíteni a felhasználók elektronikus tevékenységükkel kapcsolatos tudatosságát. A tudatosítás célja, hogy mielőtt a felhasználó bármilyen adatkezelést engedélyez, gondolja végig a lehetséges következményeket és a felhasználás lehetséges módjainak ismeretében tudatosan döntsön arra vonatkozó engedélyről vagy tiltásról. Jó, ha tudjuk, a nyilatkozat hiánya, tehát a hallgatás, a nem cselekvés nem minősül hozzájárulásnak. Amennyiben a felhasználó már megadta hozzájárulását, tudni kell, hogy az, az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre is kiterjed. A nyilatkozat vagy engedély a felhasználásra egyértelmű és könnyen átlátható legyen, hiszen egy felületesebb áttekintés esetében, adott esetben viszonylag gyorsan is dönteni tudni kell. [284]

3.5. RÉSZÖSSZEFOGLALÁS

Egy adott intézménynek elkötelezettnek kell lennie abban a tekintetben, hogy az általa megalkotott szolgáltatás vagy termék működtetéséhez szükséges adatokat az Infotv. és a GDPR által meghatározott előírásoknak vagy NAIH állásfoglalásnak megfelelően gyűjti, kezeli és tárolja. Adatkezelés esetén, az adatkezelő személyére több, és szigorúbb szabályok érvényesek, mint az adatfeldolgozás feladatának betöltésekor, hiszen az adatkezelés jellege, hatóköre, körülménye és célja, valamint a természetes személyek jogaira és szabadságaira vonatkozó, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő irányítási,

[284] Győrffyné Holló Krisztina, Dr. Leitold Ferenc: Felhasználókkal kapcsolatos információbiztonsági intézkedések kezelése a GDPR tükrében, Hétpecsétes történetek 2,5 - a GDPR antológia, Budapest, 2018.

szervezési és technikai intézkedéseket kell végrehajtani annak érdekében, hogy jogszabálynak megfelelően biztosítsa a naprakész állapotú személyes adatok kezelését. Az adatkezelés során alkalmazott technikai intézkedéseket meg kell feleltetni az adatvédelmi elveknek, különösen az adattakarékosság hatékony megvalósítása, vagy az érintettek jogainak védelméhez szükséges garanciák beépítésére vonatkozó előírások betartása érdekében. Kizárólag olyan személyes adatok kezelésére kerülhet sor, amely az előre meghatározott adatkezelési cél, jogszerűség szempontjából feltétlenül szükséges. Az adatkezelő a szabályoknak megfelelően kizárólag olyan adatfeldolgozót vehetett igénybe, aki megfelelő garanciát nyújt az adatkezelés GDPR követelményeinek való megfeleléséhez és az érintettek jogainak védelmét biztosító, megfelelő alkalmazási és technikai intézkedések végrehajtására. Az adatfeldolgozó szerződés alapján biztosítja a jogszabályi, a technikai és üzemeltetési feltételeket, és rögzíti az adatfeldolgozás tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatfeldolgozói kötelezettségeket és jogokat. Az adatkezelő és az adatfeldolgozó szervezetnek biztosítania kell a személyes adatok védelmére vonatkozó intézkedéseket, és a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettségét is. Az adatfeldolgozó szervezet az adatkezelési szolgáltatás lejárta után az együttes, egybehangzó döntés értelmében minden, a személyes adatra vonatkozó adattartalmat töröl, archivál, illetve visszajuttat az adatkezelő részére. Az adatvédelmi szabályok így a GDPR rendelkezések betartása, valamint az információbiztonsági alapelvek figyelembe vétele elősegíti az adatkezelő és az adatfeldolgozó együttműködését, a személyes adatok biztonságosabb kezelését, továbbá a bizalmasság, sértetlenség és rendelkezésre állás információbiztonság elveinek teljesíthetőségét.

Az első hipotézisem (H1) szerint feltételeztem, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és jogszabályi rendelkezések az informatikai technológiai változásokkal, továbbá a nemzetközi szabványügyi intézmények ajánlásaival és az európai szabályozással összhangban vannak, és egyben kielégítik a hazai információbiztonsági szabályozási igényeket. A jelen fejezet bemutatja az adatvédelem jelentőségét és az adatvédelmi alapelvek és szabályok alkalmazásának szükségességét, amelyet a NAIH által közzétett nyilvános határozatok alapján összeállított statisztikai adatgyűjtéssel és értékeléssel prezentáltam. Az adatvédelmi rendelkezések (GDPR, Infotv.), a NAIH határozatok, a nemzetközi és hazai adatvédelmi jogsértések esetei, valamint az esettanulmányok és a határozatok statisztikai adatainak összefüggései rámutatnak arra, hogy a második fejezetben megfogalmazott adatvédelmi és információvédelemi jogtörténet által igazolt, adatvédelemre

vonatkozó alapelvek és rendelkezések megfogalmazása és alkalmazása indokolt a papír alapú és elektronikusan tárol személyes adatok védelmének érdekében. A hazai adatvédelmi (Infotv.) és információbiztonsági (IBtv.) rendelkezések összhangban vannak a nemzetközi adatvédelmi rendelkezésekkel (GDPR).

A második hipotézisem (H2) szerint feltételeztem, hogy a felhasználói információbiztonsági tudatosság hiánya, amely az emberi tévedést és szándékos kárt eredményezhet, elősegíti az incidensek bekövetkezését, és támogatja a kiberbűnözést. A jelen fejezetben ismertetett statisztikai adatok rámutatnak arra, hogy a kiberbűnözés legfőképp az adathalászat és a káros szoftverek tekintetében jelentős mértékű, és számottevő károkat okozott, különösen az egészségügyi, oktatási, igazgatási, banki, ipari és egyéb szolgáltatóipari ágazatnak. A károk helyreállítása és a védelmi szint megerősítése jelentős anyagi ráfordítással járt, tehát gazdaságkárosító tényező. ENISA ETL jelentése szerint bár az elmúlt két évben tovább nőtt a információbiztonsági támadások száma, a hibrid irodai modell növelte a támadási felületet[285], valamint nehezítette a kibervédelmi szakemberek munkáját és az egyre növekvő felhőmegoldások alkalmazása a kiberbűnözőkre ösztönző hatással volt, ugyanakkor a szabály alapú (ISO 27001, GDPR, Infotv, IBtv. együttesen) informatikai és információbiztonsági fejlesztések, az interoperabilitási lehetőségek, a mesterséges intelligencia (MI) technológiáinak együttes alkalmazása nagyobb védelmet nyújt adatainknak, és rendszereinknek egyaránt, az egyre növekvő, kifinomult támadások kivédése ellen, továbbá az incidensek hatását (mentés és visszatöltés teszt, szimuláció, tudatosítás, router és szerver konfiguráció fejlesztése, kéretlen levelek jelölése MI módszerekkel stb.) is gyengíti. Ezen álláspont a H2 hipotézisem igazolásához is kapcsolódik, mivel igazolható, hogy az információbiztonsági rendelkezések alkalmazása hatékonyan befolyásolja az információs társadalom fejlődését.

A harmadik hipotézisem (H3), amely szerint feltételeztem, hogy a Magyarországon érvényes és intézményi adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését és a szervezet információbiztonsági tudatosság szintjét, az információbiztonsági kockázatkezelési módszerek alkalmazásával igazolható. A jelen fejezetben bemutattam az ISMS információbiztonsági kockázatkezelés elkészítésére vonatkozó szabályokat, eljárásokat és releváns módszereket, de a tényleges kockázatkezelési eljárást és vizsgálatot, valamint eredményeit a „humán faktor”, mint befolyásoló tényező jellemzésével együtt ismertetem a

[285] ENISA Threat Landscape 2021.

következő fejezetben. Az ISMS kötelező eleme a kockázatkezelés lefolytatása és a munkavállalók rendszeres információbiztonsági tudatosítása (továbbképzések, tréningek, vezetői és csoportmegbeszélések). A jelen fejezetben hivatkozott incidensek leírásával és a vonatkozó statisztikai adatokkal is alátámasztható, hogy az incidenst szenvedett intézmények jelentősebb figyelmet szentelnek az adatvédelmi és információbiztonsági követelmények betartásának és finanszírozásának, az ISMS bevezetésének és működtetésének. Az elmúlt 8-10 évben, legfőképp a támadást szenvedett kormányzati szervek és nagyvállalatok, felsőoktatási intézmények nyilatkoztak úgy, hogy a bekövetkezett incidensek után nagyobb figyelmet fordítanak az információbiztonságra és az adatvédelemre, és jobban figyelembe veszik, illetve finanszírozzák a szükséges információbiztonsági előírásokat. Tehát a vizsgálat során figyelembe vett intézményekre általában elmondható, hogy elkötelezettek az ISMS bevezetésére, az információbiztonsági szabályok szigorítására és a felhasználói biztonságtudatosság fejlesztésének támogatására. A következő fejezetben statisztikai adatokkal is igazolom, hogy a H4 hipotézis tekintetében a szervezetek által bevezetett ISMS, az információbiztonsági alapelvek és rendelkezések tudatosítása valóban hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését és a szervezet információbiztonsági tudatosság szintjét vagy sem.

4. AZ INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER SZABÁLYAI

4.1. INFORMÁCIÓBIZTONSÁGI SZABÁLYOK JELENTŐSÉGE

Jelen fejezetben az információbiztonság és információvédelem nemzetközi és hazai jelentőségét vizsgálom. A nemzetközi és hazai információbiztonsági incidensek statisztikai adatain keresztül igazolom az információbiztonsági szabványok és jogszabályi előírások intézményi szintű alkalmazásának szükségességét, a szabályok figyelmen kívül hagyásának károkozó jelentőségét, tehát a második hipotézisem (H2) bizonyításának kiberbűnözés összetevőjét. Tekintettel arra, hogy az információbiztonság megerősítésére vonatkozó előírások megfogalmazása és intézkedések végrehajtása nemcsak a magánvállalkozásokat, vagy az állami intézményeket érinti, hanem egész nemzetünk érdeke, ezért kiindulópontja nem lehet más, mint az államigazgatás és a közigazgatás. Ma már nemcsak az állami intézmények vagy a vállalkozások használják azokat a közszolgálati információs rendszereket[286] [287] [288], amelyek jelentősen hozzájárulnak a közigazgatás hatékony működéséhez, hanem a magánszemélyek, mint általános felhasználói réteg, rendszeresen igénybe veszik állampolgári kötelezettségük teljesítéséhez, továbbá a tanuláshoz vagy az oktatáshoz. Véleményem szerint a közszolgálati információs rendszereknek a közigazgatási célkitűzéseken, hasznosságon túl egyszerre kell teljesítenie az adatvédelmi, információbiztonsági, kibervédelmi és interoperabilitási alapelveket és előírásokat. A vizsgálat során elsődlegesen az információbiztonsági incidensek statisztikai adatain, az információbiztonsági irányítási rendszer bemutatásán és alkalmazhatóságán, valamint az információbiztonsági kockázatkezelésen keresztül szemléltetem az információbiztonsági (IB) szabályok betartásának szükségességét. Továbbá arra is szeretnék rávilágítani, hogy az IB szabályok alkalmazása minden olyan informatikai rendszerben szükséges, ahol jelentős mértékű személyes vagy értékes üzleti, ipari, kutatási adatot kezelnek vagy biztonsági mentés céljából tárolnak, illetve az adott rendszer segítségével továbbítanak. A kutatásom során vizsgált nemzetközi és hazai információbiztonsági incidensek

[286] Kőnig Balázs, A közigazgatási információ-rendszerek fejlesztésének jogi környezete és vezetési intézményei, Informatikai rendszerek a közszolgálatban I., Scientia Rerum Politicarum, Sorozatszerkesztők: Kiss György és Kis Norbert, Szerkesztette: Sasvári Péter, Dialóg Campus, Budapest, 2020.
[287] Krasznay Csaba, A közigazgatás IKT-infrastruktúrája és technológiaelemei, Informatikai rendszerek a közszolgálatban I., Scientia Rerum Politicarum, Sorozatszerkesztők: Kiss György és Kis Norbert, Szerkesztette: Sasvári Péter, Dialóg Campus, Budapest, 2020.
[288] Tarpai Zoltán, SZEÜSZ-ök – Koncepció és példák, Informatikai rendszerek a közszolgálatban II., Scientia Rerum Politicarum, Sorozatszerkesztők: Kiss György és Kis Norbert, Szerkesztette: Sasvári Péter, Dialóg Campus, Budapest, 2020.

statisztikai adatai rámutatnak az információbiztonsági kockázatkezelés szempontjából kezelendő területekre. A kutatásom során figyelembe vettem a GDPR és az Infotv. életbe lépését, és külön vizsgáltam az ez előtti, illetve utáni időszakot, valamint időszak tekintetében figyelembe vettem a Covid-19 világjárvány, illetve a fokozottabb távmunka és az információbiztonsági események egymásra gyakorolt hatását, következményeit. A kutatásomhoz nemzetközi és hazai tudományos publikációk, hatóságok és információbiztonsággal foglalkozó nagyvállalatok által nyilvánosságra hozott, hiteles statisztikai adatokat vizsgáltam, annak érdekében, hogy különösen a második (H2) és harmadik (H3) hipotézisem információbiztonsági tényezőit igazolni vagy cáfolni tudjam. A fejezetben található kutatási eredmények közléséhez és a háttérkutatáshoz dokumentum- és tartalomelemzési, kvalitatív, minőségirányítási, különösen információbiztonsági és kockázatkezelési módszereket, összehasonlító, statisztikai valamint adatelemzéseket, továbbá empirikus kutatást, a matematikai logika alkalmazásával használtam.

4.2. INFORMÁCIÓBIZTONSÁGI KONTROLLOK ÖSSZEFÜGGÉSEI, PREVENTÍV ÉS KORREKTÍV INTÉZKEDÉSEK

Magyary Zoltán, *a közigazgatás gazdaságosságának és eredményességének fokozása nem kívánja a jogállamiság feladását*[289] [290] [291] gondolatával összefüggésben megállapítható, hogy a közigazgatás, működése és intézkedések szempontjából egyszerre lehet eredményes, hatékony és jogszerű is. A közigazgatás tevékenységeihez ma már hozzátartozik az adatvédelmi szabályozás, a kibervédelmi szabályozás és teljesülésük hatósági felügyelete. Információs világunkban az adatvédelmi szabályok megfelelő alkalmazását, a kibervédelmi szabályok és gyakorlati intézkedések egészítik ki. A közigazgatási alrendszerek eredményes együttműködése hatékonyságnövelő, hiszen *a közigazgatás sajátos igazgatás, amelyben a tudományos munkaszervezés és üzemvezetés törvényszerűségei alkalmazhatók, ezáltal hatékonysága és gazdaságossága hallatlan mértékben növelhető.*[292] Ezen gondolatokat

[289] Magyary Zoltán, A Magyar Közigazgatás gazdaságosságának és eredményességének biztosítása, A M. Kir. Miniszterelnök Úr elé terjesztett javaslat, Budapest, 1931.
[290] Magyary Zoltán, A Magyar Közigazgatás racionalizálása, Budapest, 1930.
[291] Varga Zs. András, 4. Jogállamiság, Jogállamiság-paradigma a XIX. század elején, (Csink Lóránt, Schanda Balázs, Varga Zs. András, A magyar közjog alapintézményei, Budapest, Pázmány Press, 2020.)
[292] „*Az eredmények fokozásának szükséglete vezetett minden téren, gazdaságban és közigazgatásban egyaránt a régi megoldások revíziójára, hatékonyság és gazdaságosság (efficiency) tekintetében való mérlegelésére, a régi tökéletlen eljárások és megoldások helyett észszerűbb, új megoldások bevezetésére, a tradíció helyett a ráció érvényesítésére és így foglalta el a takarékosság helyét a racionalizálás.*" „*Magyarországon a racionalizálási mozgalom lassabban hódít tért. Egyelőre csak a normalizálás céljára rendelkezünk szervezettel.*"
Magyary Zoltán, A Magyar Közigazgatás racionalizálása, Budapest, 1930.

figyelembe véve, véleményem szerint a közigazgatás-tudomány kutatás szempontjából az adatvédelmi szabályozás mellett az információbiztonsági és kibervédelmi szabályokat is vizsgálni kell. A vizsgálathoz hozzá tartozik a jogtörténet, az adatvédelem és kibervédelem területéhez tartozó esetvizsgálat, adatvédelmi és információbiztonsági incidensek statisztikai adatai, esetszámok és okozott kár mértéke. Az esetszámok és az okozott kár mértéke determinálja az adatvédelmi és információbiztonsági szabályok módosításának, modernizálásának szükségességét. Amennyiben nem ismertek a technológiai és az incidensek következtében összegyűjtött statisztikai adatok, úgy nehezebb pontosítani a szabályokat is. Az adatvédelmi és információbiztonsági alapelvek útmutatóul szolgálnak a szabályok finomításában. Tehát jogalkotás szempontjából mindkét terület jelentős. A továbbiakban található információbiztonsági statisztikai adatok, valamint Európai Uniós valamint hazai rendelkezések bemutatásával szemléltetem az információbiztonsági rendelkezések jelentőségét. Sajnálatos módon csak a közszolgálati rendszerekre vonatkozik az állami és önkormányzati szervek elektronikus információbiztonsági előírásai az Ibtv., így a vállalkozások számára csak az Infotv. szabályai érvényesíthető, az elektronikus információbiztonsági szabályok kiterjesztése egyelőre még nem. A Világgazdasági Fórum éves, globális kockázati rangsorában az eddig ismert megszokott fenyegetések, úgymint a gazdasági, a környezeti, a politikai, a társadalmi, de különösen a háborús konfliktusok, terrorizmus, természeti katasztrófák mellett megjelent, majd egyre nagyobb teret követel magának a technológiai, úgymint a kibertér fenyegetései (Risk Cyber Dependency). Az elmúlt években a NATO kibervédelmi központja, az ENSZ Nemzetközi Távközlési Egyesülete (ITU), és többek között az ENISA, így az Európai Unió különböző szervezeti szinteken, ajánlások, stratégiák és irányelvek által hívták fel a figyelmet arra, hogy a minimális feltételek és intézkedések elengedhetetlenek a kibertér biztonságának minimális szinten tartásához. Az ENISA feladata, hogy fokozza az operatív együttműködést uniós szinten, segítse az uniós tagállamokat kiberbiztonsági incidenseik kezelésében, támogassa az EU koordinációját nagyszabású, határokon átnyúló kibertámadások és válságok esetén, és ennek érdekében megalkották a hálózati és információs rendszerek biztonságáról szóló irányelvet (NIS irányelv).[293] A NIS irányelv felülvizsgálata alapján meghatározott és 2020. december 16-án benyújtott új jogalkotási javaslat (NIS2 irányelv), amely korszerűsíti a meglévő jogi keretet, figyelembe véve a belső piac digitalizálódását és az információbiztonsági fenyegetettség alakulását. A

[293] Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148, letöltés: 2022. február 26.

társadalom digitális átalakulása, amelyet a COVID-19 világjárvány által megnövekedett online munkavégzés és oktatás fokozta és kibővítette az online fenyegetettséget és incidenseket, ezáltal az európai ügynökségek fokozottabb, adaptált és innovatív válaszaira van szükség.[294] A kibertér védelme nemcsak a nemzetbiztonságot érinti, de hatással van a nemzet gazdaságára, társadalmára, kihat az informatikai és kommunikációs hálózatok minden részvevőjére, a nemzetközi, az állami vagy a civil szereplőkre, amely egy adott esetben egy lehetséges célponttá, illetve áldozattá válhat. Az Európai Parlament és Tanács 2019/881 számú rendeletében kibertámadások és –fenyegetések növekedésének problémáját, és kezelésére vonatkozó tagállami és Uniós intézkedési igényeket fogalmazott meg. [295] A rendelet iránymutatása által a kiváltó okok és következmények, a lehetséges legteljesebb kockázati tényezők palettáját, azontúl az objektumok és egyéb szereplők sebezhetőségének, támadhatóságának vizsgálatát célszerű elvégezni mind civil, állami, valamint nemzetközi szintéren. A kibertámadások elleni megelőzések és védekezések, elhárítás része a kiberbiztonság valamely elvárt szintű fenntartásának. A preventív megelőzések tekintetében kiemelten fontos szerepet játszik az ISO által kiadott ISO/IEC 27000-es információbiztonsági irányítási rendszer szabványcsaládjának, az Európai Unió által megalkotott információbiztonsági irányelveknek való megfelelés, és a szervezet szintű alkalmazás. Az informatikai védelmi rendszerek kialakításánál a vonatkozó informatikai szabályozások és a rendelkezésre álló technikai megoldások együttes figyelembe vétele és alkalmazása szükséges. A támadás elleni védekezések nem merülnek ki az Európai Uniós, illetve a hazai szabályozási rendszerrel. Az EU-s irányelvek és a törvényi szabályok iránymutatással és előírásokkal segíthetik elő a preventív intézkedéseket. A kiberbűnözés által okozott jelentős mértékű anyagi

[294] Shaping Europe's digital future, Proposal for directive on measures for high common level of cybersecurity across the Union, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union, letöltés: 2021. április 24.

[295] „*Egyre gyakoribbak a kibertámadások, és az összekapcsoltság következtében a kiberfenyegetéseknek és -támadásoknak egyre kiszolgáltatottabbá váló gazdaság és társadalom fokozottabb védelmet igényel. Míg a kibertámadások általában nem ismernek országhatárokat, a kiberbiztonsági és bűnüldöző hatóságok hatásköre és szakpolitikai válaszintézkedései túlnyomórészt nemzeti szintűek. A nagyszabású biztonsági események az egész Unióban megzavarhatják az alapvető szolgáltatások nyújtását. Ezért hatékony és összehangolt uniós szintű reagálásra és válságkezelésre van szükség, melynek alapját célirányos szakpolitikai intézkedéseknek és az európai szolidaritást és kölcsönös segítségnyújtást szolgáló gazdagabb eszköztárnak kell képeznie. Emellett a szakpolitikai döntéshozók, a gazdasági élet szereplői és a felhasználók számára egyaránt fontos, hogy megbízható uniós adatok alapján rendszeres értékelés készüljön az EU kiberbiztonságának és kiberellenálló képességének mindenkori helyzetéről, továbbá szisztematikus legyen a jövőben várható fejlemények, kihívások és fenyegetések előrejelzése uniós és globális szinten egyaránt*."
Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), letöltés: 2022. február 28.

kár is azt mutatja, hogy nem elég csupán a védekezéssel és az elhárítással foglalkozni. „*Az információ megfelelő védelem nélkül ellenőrizetlen az adatok kiszivárgása, az átgondolatlan, ellenőrizetlen módosítások adatvesztést okozhatnak, nyomnélküli adatvesztés esetén kicsi a helyreállíthatóság esélye. az információk nem érhetőek el akkor, amikor szükség van rájuk.*”[296]

4.2.1. AZ INFORMÁCIÓBIZTONSÁGI FENYEGETÉSEK, A PREVENTÍV INTÉZKEDÉSEK JOGALAPJA

Az európai és hazai szabályok kinyilatkoztatásával és alkalmazásával, a technikai megoldások és szabályok használatával sem lehet minden esetben a támadási kísérleteket teljes mértékig visszaszorítani, illetve megelőzni az incidenseket. Teljes mértékű informatikai védelem nem létezik. A kiberbűnözés célja többféle lehet. Az információs rendszerek ellen elkövetett támadások legfőképp arra irányulnak, hogy megzavarják vagy gátolják az adott szervezetek, rendszerek működését, ezáltal nagyfokú, elsődlegesen anyagi kárt okozzanak vagy információt tulajdonítsanak el. A támadások túlnyomó részét politikai és/ vagy vallási aktivisták, gazdasági-bűnözői csoportok, terrorista szervezetek, vagy egyes államok titkosszolgálat szervezetei követik el. A kiberbűnözés okozta kár a világgazdaságban már jelentős értékeket mutat, amely 2014-ben átlagosan 445 milliárd USD összeget jelentett, a becslések szerint az éves tényleges kár ennek mértékét jóval meghaladja.[297] Ebből az Amerikai Egyesült Államok kanyarított a legtöbbet, amely 108 milliárd USD, de mögötte Kína (60 USD) és Németország (59 UDS) is jelentős értékeket mutatott fel. A kimutatások szerint az úgynevezett Carbanak-csoport 2015. évi felfedezéséig vélhetően közel két év alatt 30 ország 100 pénzintézetétől, egy milliárd dollárt meghaladó összeget tulajdonított el. Ma már bűncselekmény kategóriába tartozik a jelentős károkat okozó célzott adatlopás, amelyek száma évről-évre növekszik. Természetesen csak megbecsülni lehet, mekkora kárt okozhat a globális gazdaság számára a kiberbűnözés. A Cybersecurity Ventures 2016. évi elemzése alapján, 3 billió dollárra becsülik a 2017. évi károsszeget. A kimutatásba beleszámították a direkt és indirekt káreseményeket is, tehát a személyes adatok kiszivárogtatása okozta kárt, üzleti titkok nyilvánosságra kerülését, vagy az (kritikus) infrastruktúrák sérülését.[298] 2018. egy olyan év volt, amely jelentős változásokat hozott a számítógépes fenyegetettségben, és a kibertámadások száma 2019-ben tovább nőtt. Az

[296] Muha Lajos, Szádeczky Tamás, Irányítási rendszerek, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, 2014.
[297] Kiberfenyegetések és kibervédelem, Országgyűlés Hivatala, Infojegyzet, 2016/44., Budapest, 2016. szeptember 29. .
[298] Kiss Attila, Krasznay Csaba, A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai, Információs Társadalom, XVII. évf. (2017) 1. szám

Egyesült Állomok Stratégiai és Nemzetközi Tanulmányok Központjának (CSIS) 2017. évre vonatkozó felmérése alapján megállapították, hogy globális szinten a számítógépes bűnözés által okozott kár mértéke csaknem 608 billió USA dollár. Megállapították továbbá, hogy a kár mértéke 3 év alatt 150 billió USA dollárral nőtt, ami önmagában is tetemesnek mondható. A költségek nagy része az Egyesült Államokat terheli, de például Németországban veszteségként 64 billió USA dollárt mutattak ki, ami az előző, 2014. évi felmérési adatokhoz képest 5 billió USA dollárral nőtt. A felmérések azt is megmutatták, hogy a bankszektor, pénzügyi szolgáltatók és az egészségügyi ágazat viselte a legtöbb számítógépes bűnözéssel kapcsolatos költségek jó részét. Az információbiztonsági szakemberek részéről sikerült a támadások nagy részét kivédeni, köszönhető ez a technikai- és a tudásfejlődésnek is. Az aktív védekezés elemeként megjelenő profilozás, a támadási gyakorlatok és a rosszindulatú programok hatékonyabb azonosításához, ezáltal hatékonyabb védekezési technikákhoz és elhárítási arányokhoz vezetett. A kezdeti sikereket a számítógépes fenyegetések intelligenciájának (CTI - Cyber threat intelligence) és a hagyományos intelligenciának a kombinálásával érték el. Ez egyértelműen jelzi, hogy a kiberfenyegetés-intelligenciát meg kell nyitni más kapcsolódó tudományterületek felé az értékelések és a hozzárendelés minőségének javítása céljából. A 2018. évi kiberfenyegetettség fő tendenciái szerint, még mindig a rosszindulatú e-mail és az adathalász üzenetek állnak az első helyen, valamint az automatizált támadások és a programozott eszközök segítik elő a támadások sikerességét. Az alacsony szintű IoT-eszközök és szolgáltatások hiányzó védelmi mechanizmusai elősegítik az incidenseket, ezért az ENISA szervezete is sürgeti a mielőbbi megoldásokat és a hatékony gyakorlati megvalósítást, mivel az alacsony képességű szervezetek, illetve végfelhasználók számára a kiberfenyegetés-elhárítási megoldások hiányával a gazdaság szereplőinek ugyanúgy foglalkoznia kell, nemcsak az adott kormánynak. Nemcsak az Európai közösség, de Amerika és a Távol-Kelet is napi szinten küzd a különböző irányból érkező incidensek ellen, egyre fejlettebb IT szabályokkal, technológiával és kibervédelmi szakember csapat segítségével. A kibertér és a való világ határai kezdenek összemosódni. Erre mutat rá egy szingapúri kormányzati döntés, amely értelmében immár a térfigyelő kamerák adatbázisát, a banki adatbázisokat, valamint a kormányzati hivatali adatbázisokat összekötnék és az adatokat egységes bűnüldözői rendszerben használnák fel. Az Ipar 4.0 teret hódít, és a fejlesztés nem állhat meg. Szingapúr törpeállama számos technológia terén a világ egyik legambiciózusabb állama, így érthető, hogy jelen esetben az információbiztonságra vonatkozó biztosítékot maga a GovTech cég vállalta. Nyilatkozatuk alapján, az alkalmazás sikeressége mögött az emberi arcok felismerésének valódisága áll, amely

miszerint az arcok mögött valós személyek lesznek, valós karakterrel, nem pedig egy retusált kép. A technológiát integrálják az ország digitális azonosítási rendszerébe, amelyet összekötnek az adóhatósággal is. Így a bűnüldözői tevékenységet kiterjesztik más funkciót ellátó térbe is. Számos magánvállalkozás és pénzintézet is segítheti a projekt megvalósulását. A nagymértékű digitális fejlesztésnek árnyoldalai is vannak, némi ellentmondással a háttérben, miszerint hogyan egyeztethető össze és feleltethető meg a gyakorlatban az interoperabilitási elvekkel, a különböző informatikai rendszerek együttműködésével, az adatvédelmi szabályozással, az etikai alapelvekkel és az információbiztonsági előírásokkal, valamint az egyének reakciójával. A felhasználói közösség érti a bűnüldözés fontosságát, de a társadalmat valóban az ember bűnözői hajlamának oldaláról kell vizsgálni vagy lenne erre más módszer is, mint például a technikai és információbiztonsági módszerek alkalmazása, a társadalom tudatosítása, jogi és önvédelmi módszerek kifejlesztése és alkalmazása a kibertérben és a nyilvános tereken egyaránt. [299] Ebben a fejezetrészben a fenyegetéseken és információbiztonsági incidenseken keresztül szemléltetem azokat az incidenstípusokat, amelyek napjainkban is károsítják információs eszközeinket, működési nehézségeket, informatikai problémákat, rendkívüli szolgáltatáskimaradást és esetlegesen adatvesztést, adatszivárgást okoznak. A kutatás során az elmúlt 8-10 év nemzetközi és hazai információbiztonsági incidensek és statisztikai adatait vettem figyelembe, valamint elkülönítettem a GDPR és az Infotv. rendelkezéseinek életbe lépése előtti és utáni időszakot, és figyelembe vettem a Covid-19 világjárvány információbiztonságra gyakorolt hatását. A kutatáshoz megvizsgáltam nemzetközi és hazai tudományos folyóiratok, kormányzatok és információbiztonsággal foglalkozó nagyvállalatok által közzétett, hiteles statisztikai adatokat, amelyeket a következő alfejezetekben részletezek.

4.2.1.1. AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEK STATISZTIKAI ADATAI (2015-2018)

Az információs eszközöket ért támadás vagy támadási kísérlet a sebezhetőségeket, gyenge pontokat használják ki, és a káros tevékenységet nem állítja meg az országhatár. Nemcsak az európai országokat ért támadási kísérlet érhet célba. Az amerikai Nemzetbiztonsági Hivatal (NSA) annak ellenére, hogy részt vett különösen a Windows 7 fejlesztésében is, 2016-2017-ben mégis gondjai adódtak a felügyeletére bízott információk védelmével kapcsolatban. Amennyiben teljes mértékben hinni lehet az internetes információknak, a megjelent híradások szerint, mintegy 100 GB információ szivárgott ki a szervezettől. Az elmúlt évben a Shadow

[299] Győrffyné Holló Krisztina, Az információbiztonsági tudatos viselkedés az incidensek elkerülésének egyik tényezője, DUNAKAVICS 8 : 12 pp. 5-18. , 14 p. 2020.

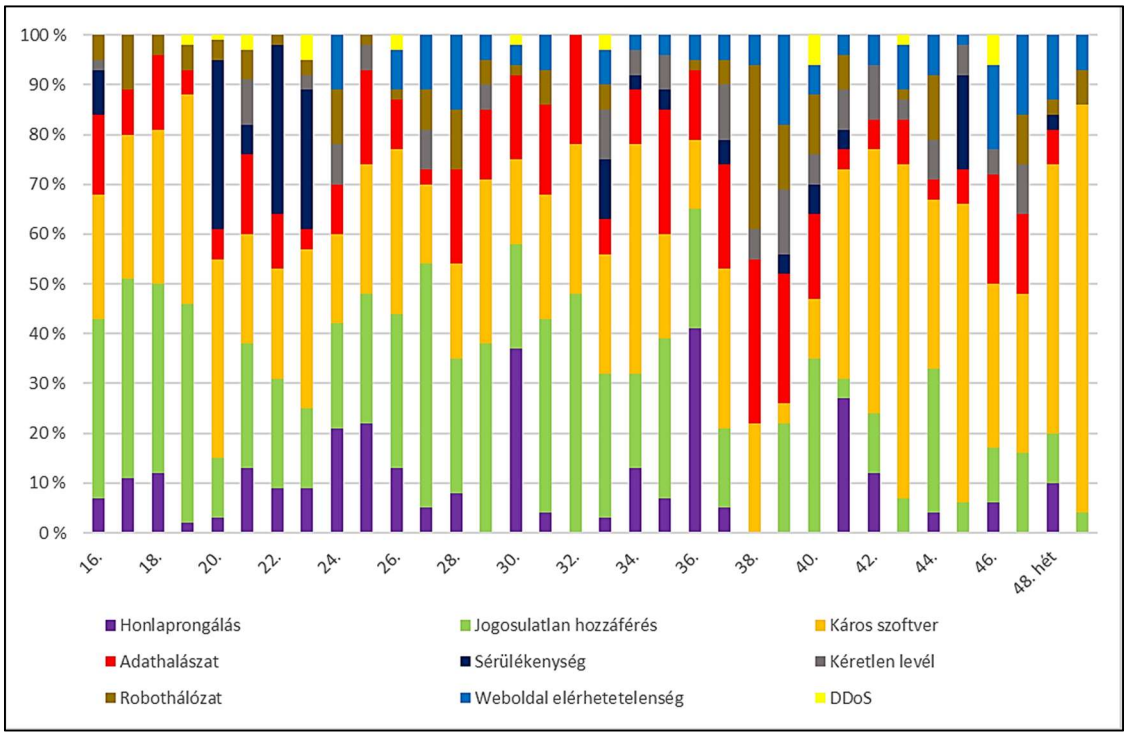
Brokers hackercsapat közvetett közreműködésével több millió dollár értékben próbálták árulni a kritikus, NSA szervezetétől megszerzett információkat.[300] Az egyik ismertebb adateltulajdonítást 2015. februárjában fedezték fel, melynek során az Anthem amerikai egészségbiztosító cég informatikai rendszerének feltörésével közel 80 millió ügyfél személyes adatát tulajdonították el.[301] A Symantec információi[302] szerint a támadást elkövető Black Vine nevű hackercsoport 2012 óta több más ipari és kormányzati szervezet informatikai rendszerét is megtámadta. A támadássorozatok kritikus rendszereket is érintettek, mint például a lengyel nemzeti légitársaság, az ukrán elektronikai hálózat, a kijevi nemzetközi repülőtér, vagy egy németországi atomerőmű informatikai rendszerében is támadások nyomait, azaz kártékony kódokat fedeztek fel. A kísérletek és az események a kormányzati szférát sem kímélték, így kibertámadás érte a Bundestag hálózatát[303], a svájci állami haditechnikai céget[304], valamint a Pentagont, a Fehér Házat, vagy az Amerikai Egyesült Államok állami szervezeteit[305]. A támadási típusok között megtalálható a DDoS (Distributed Denial of Service) [306], amely tipikus túlterheléses és elosztott szolgálttatás megtagadás típusú támadás. Az ENISA 2016. januári jelentése[307] is megerősítette, hogy 2014-15. években a kiberkémkedés, a káros szoftverek, a web-alapú és túlterheléses támadások száma tovább növekedett. A magyar Kormányzati Eseménykezelő Központ információi alapján évek óta komoly problémát jelentenek a zsarolóvírusok, mint például a ransomware és a WannaCry, vagy az ExPetr.. A napjainkban is terjedő, célzott támadási módszer a hamis, adatbányász mobil alkalmazások, illetve azok népszerűsítése és terjesztése vagy a kriptobányászathoz szükséges számítási erőforrást megszerezzék.[308] Az lakosság mobil erőforrásaink megszerzésére irányul egy hamis kriptovaluta tőzsdei mobil alkalmazás. Az alkalmazás segítségével a kiberbűnözők a kriptovaluta forgalom alapját képező kriptovaluta bányászathoz szükséges erőforrást szeretnék

[300] International cyber law, The Shadow Brokers publishing the NSA vulnerabilities (2016)
[301] California Department of Insurance, Anthem Data Breach, (2015)
[302] Jon DiMaggio. The Black Vine cyberespionage group, Symantec, 2015.
[303] Európai Unió Tanácsa és az Európai Tanács, Rosszindulatú kibertámadások: uniós szankciók a Bundestag elleni 2015-ös kibertámadásért felelős két személlyel és egy szervvel szemben (2020.)
[304] Information Assurance, Situation In Switzerland And Internationally, Federal IT Steering Unit FITSU, Federal Intelligence Service FIS, Reporting and Analysis Centre for Information Assurance MELANI, 2016.
[305] Zachary Figueroa, Time to Rethink Cybersecurity Reform: The OPM Data Breach and the Case for Centralized Cybersecurity Infrastructure, 24 Catholic University Journal of Law and Technology, USA, (2016). https://scholarship.law.edu/jlt/vol24/iss2/7, letöltés: 2022. február 26.
[306] The World Wide Web Security FAQ, W3, https://www.w3.org/Security/Faq/wwwsf6.html, letöltés: 2022. február 26.
[307] ENISA Threat Landscape 2015.
[308] ESET, A kiberbűnözők fertőzött weboldalakat használnak a kriptovaluták bányászatára ESET, hírek, https://www.eset.com/hu/rolunk/hirek/sajtokoezlemenyek/hogyan-lehetsz-tudtodon-kivul-kriptobanyasz/, letöltés: 2022. február 26.

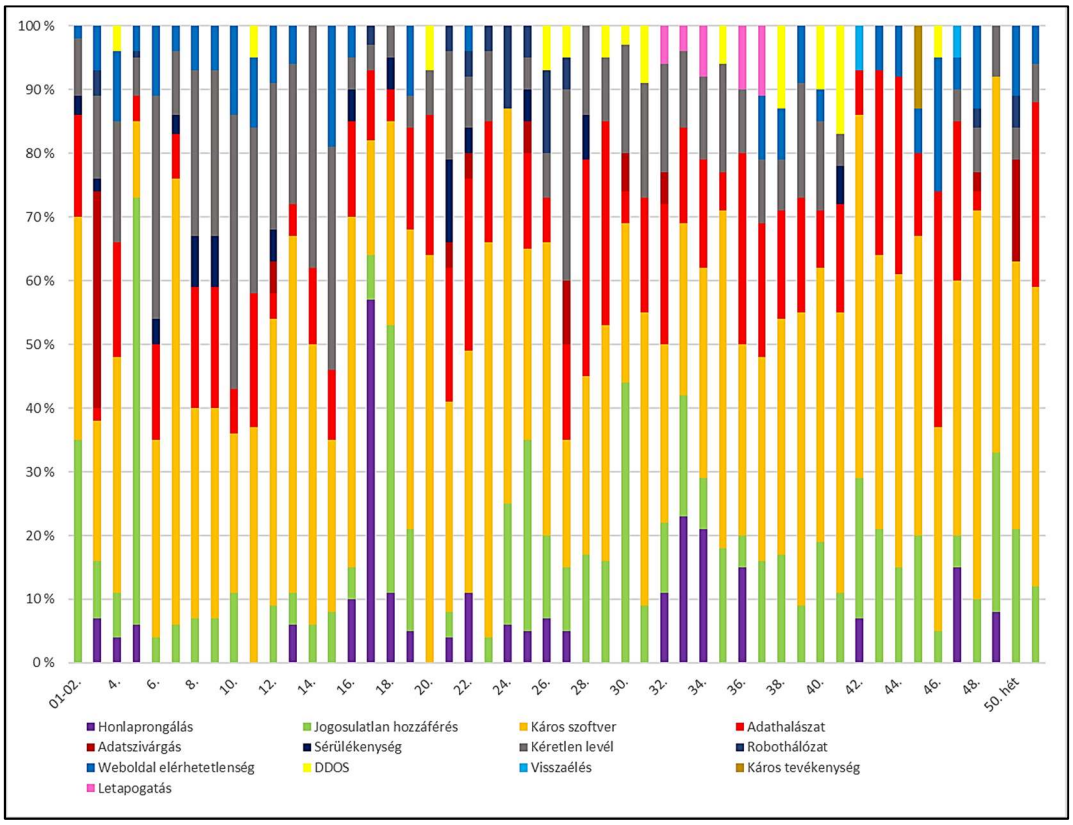
megszerezni. 2017. szeptemberében a támadók rosszindulatú scriptet juttattak be a videómegosztó, és a böngészőben futó játékoldalakba. Az adatbányászathoz szükséges számítási erőforrást megszerezték a biztonsági réssel rendelkező, feltört IT eszközökön futó böngészőkön keresztül. A népszerű Poloniex kriptovaluta tőzsde felhasználói váltak adateltulajdonító alkalmazások célpontjaivá és áldozatává. A hamis mobilprogram hivatalos Poloniex mobilalkalmazásnak álcázva magát tűnt fel a Google Play hivatalos áruházában. A kibertámadók a kriptovalutához kapcsolódó belépést szolgáló kódok eltulajdonítása mellett még a felhasználók Gmail fiókjainak hozzáférését is megpróbálták megszerezni. A kártevőket tartalmazó alkalmazásokat a szakemberek jelzése után eltávolították az áruházból, de így is közel 5 500 felhasználó már telepítette a programokat. Az incidensnél mivel nem volt hivatalos mobilalkalmazás, ezt a lehetőséget használták ki a kiberbűnözők, visszaélve a szervezet nevével folyatták tevékenységüket.[309] A 2017. évi 49. számú NBSZ NKI IT-biztonsági sajtószemle[310] incidens adatai szerint: 2017.12.06. és 2017.12.12. közötti, karácsony előtti időszakot tekintve az incidensek eloszlása kockázati besorolás szerint 39%-a alacsony, 61%-a közepes, továbbá támadástípusok eloszlása szerint 4%-a jogosulatlan hozzáférés, 7%-a robothálózat, 7%-a weboldal elérhetetlenség, 82%-a káros szoftver alapú volt. Az NBSZ NKI által közzétett támadástípusok 2017-2018. év heti eloszlását a következő ábrák szemléltetik, amely alapján megállapítottam, hogy a hazai statisztikai adatok is megerősítik azt a tényt, miszerint ebben az időszakban a legelterjedtebb támadástípus a káros szoftver, a jogosulatlan hozzáférés és az adathalászat volt. (6. ábra)

[309] ESET, Az erőforrásaink megszerzése miatt feltört gépek után, most hamis kriptovaluta tőzsdei alkalmazás tűnt fel a Google Play áruházban, ESET, hírek, https://www.eset.com/hu/hirek/kriptovaluta-elleni-bunozes/ , letöltés: 2022. február 26.

[310] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, IT-biztonsági sajtószemle, https://nki.gov.hu/it-biztonsag/kiadvanyok/sajtoszemle/, letöltés: 2022. augusztus 7.

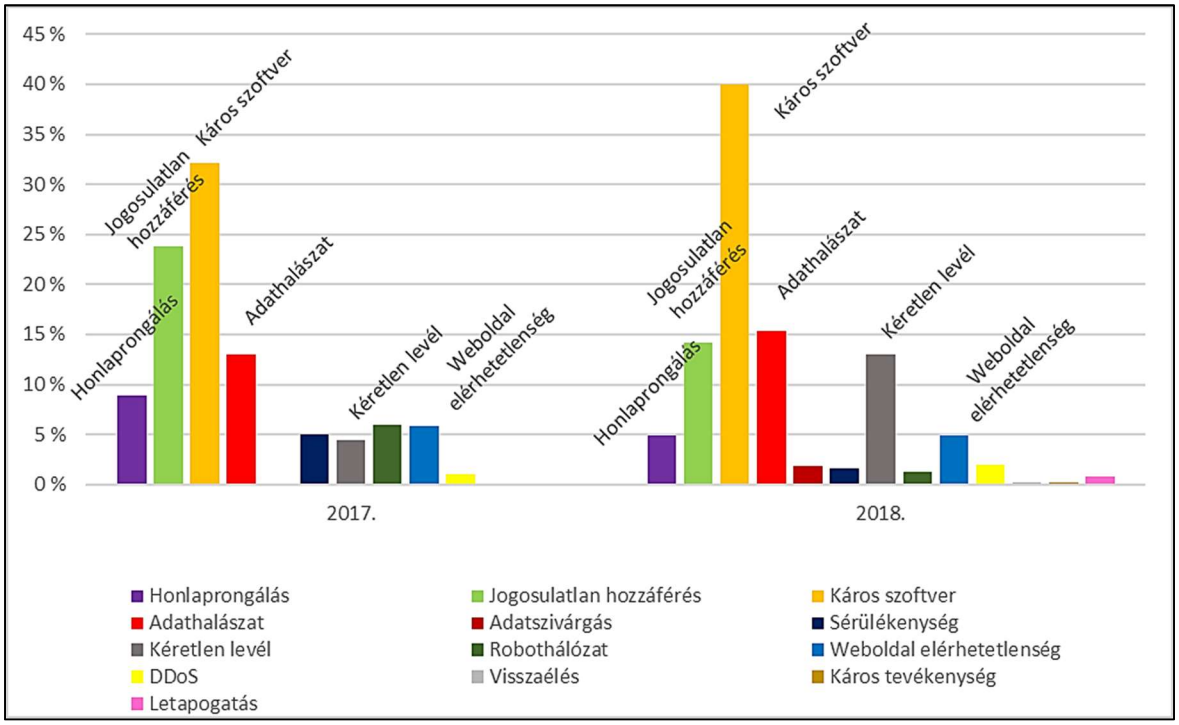


6. ábra, Támadástípusok eloszlása NBSZ NKI statisztikai adatai alapján – 2017. 16-49. hét saját adatgyűjtés, vizsgálat alapján saját szerkesztés



7. ábra, Támadástípusok eloszlása NBSZ NKI statisztikai adatai alapján – 2018. 1-51. hét saját adatgyűjtés, vizsgálat alapján saját szerkesztés

További információbiztonsági incidenst okozott a weboldalak ellen indított támadás (honlaprongálás, weboldal elérhetetlenség) vagy a felhasználókat célzó kéretlen levélhadjárat és következményei. A 2017. és 2018. évi adatokat összevetve, a káros szoftverek vezették a ranglistát, és 2018-ban a támadástípusok arányát tekintve kiegyenlítődött a jogosulatlan hozzáférés, az adathalászat és a kéretlen levelek aránya. (7., 8. ábra) Ezen utóbbi típusok aránya összesen eléri a káros szoftverek arányát, tehát a felhasználókat célzó támadások száma jelentős mértékű. A felhasználókat ért támadási kísérlet eredményessége és az incidens bekövetkezése azon múlik, hogyan reagál a felhasználó az adott próbálkozásra. Közvetett módon pedig megállapítható, hogy információs rendszereink védettsége több, mint 40%-ban múlik a felhasználói reakción, a felkészültségen és a biztonságtudatos viselkedésen. A *felhasználók* meghatározásához természetesen az adott információs rendszerben kiadható összes szerepkört figyelembe vettem, az olvasási joggal bíró úgymond nézegető szerepkörtől az alkalmazás, az adatbázisszervert, az operációs rendszert, illetve a hálózatot üzemeltető legmagasabb szintű jogosultságig.



8. ábra, Támadástípusok eloszlása NBSZ NKI statisztikai adatai alapján – 2017-2018.

saját adatgyűjtés, vizsgálat alapján saját szerkesztés

A támadástípusok százalékos elosztásának vizsgálatához elengedhetetlenül szükséges, hogy ismerjük a kártényezők mértékét, ebben az esetben az adatszivárgás vagy adatlopás adatmértékét. A következő statisztikai felmérés és vizsgálat központjában az az adatmennyiség

áll, amely egy-egy incidens során veszélybe kerül vagy elvész, tehát az alábbi kutatásom eredménye rávilágít arra, hogy a kibertámadások mekkora adathalmazt érintenek. A felsorakoztatott esetek és statisztikai adatok csak többé-kevésbé kapcsolódnak a közszolgáltatás rendszereihez, mégis a tapasztalatok alapján célszerű bővíteni az elektronikus ügyfélkezelési rendszerhez, például a kormányzati, illetve a *magyarország.hu* portálrendszerhez kapcsolódó mobil operációs rendszer által támogatott, a kormányablak tevékenységeihez kötött mobil applikációs rendszerek információvédelmi és -biztonsági szabályait. Ebben az esetben legfőképp a megelőző, védelmi intézkedésekre kell fókuszálni. A közszolgálati rendszerekben okozott, egy-egy támadási kísérletnek, vagy incidensnek komoly gazdasági és személyi, valamint politikai és nemzetvédelmi vonatkozása lehet. A magyar biztonsági kutatók nemcsak a hálózati- vagy végpontvédelmet, vagy a mobil eszközök védelmét, hanem ma már az okostévé gyártói illetve az internetes hozzáférés alapján az elektronikus világ felé nyitott kapcsolatokat is vizsgálják. A gyártó felé küldött adatbekérés a nézők, illetve a használók tudta, illetve előzetes engedélye nélküli információszerzésnek minősül. Bár a gyártók esetleges frissítéssel korrigálni tudják a hibát[311], teljes mértékig a felhasználó csak akkor tud megbizonyosodni az e fajta adatáramlás megszűnéséről, ha internetkapcsolat sincs. Nemcsak a gyártókat érdekli az smart tévék adattartalma, hanem a hackereket is. Az informatikai technológia és megoldás fejlődésével lehetőségünk van napi szinten használni biometrikus adatainkat, ugyanakkor egy-egy adatvédelmi incidens felhívja a figyelmet az adatvédelmi beállítások szigorítására. A szingapúri hatóságok profilozó, arcfelismerő rendszerének használata némi ellenvéleményt eredményezett. Általában megállapítható, hogy a magáncélra felhasználható IP kamerák legtöbbször nem rendelkeznek megfelelő biztonsági beállítással, így a laptophoz vagy PC-hez csatlakoztatva, beállítás nélkül használhatja a felhasználó. A biztonsági kamerák ezzel ellentétben komolyabb konfigurációs beállítási lehetőséggel rendelkeznek, de ez nem jelenti azt, hogy a nap 24 órájában figyelik, vagy logelemzést végeznek a rendszergazdák. A hackerek tudásán, ügyességén és leleményességén is múlik, mikor és hogyan használják ki a biztonsági réseket. [312] A fejlesztési törekvések szembe állíthatók egy szintén szingapúri hírrel, amely szerint egy hacker csoport több, mint 50000 otthoni IP kamera feltörésének incidensét vállalták

[311] Nem kémkednek tovább az LG okostévéi, 2013. november 22., https://pcworld.hu/eletmod/nem-kemkednek-tovabb-az-lg-okostevei-141629.html, letöltés: 2021. december 10.
[312] Győrffyné Holló Krisztina, Az információbiztonsági tudatos viselkedés az incidensek elkerülésének egyik tényezője, DUNAKAVICS 8 : 12 pp. 5-18. , 14 p. 2020.

magukra.[313] [314] A hacker csoport szélhámosai 150 USA dollárért cserében hozzáférést biztosítanak az IP kamerák által felvett teljes gyűjteményhez. A helyi *The News Paper* szerint már legalább 70 előfizetője van gyűjteménynek és a csoportnak legalább 1000 tagja van világszerte. A megosztott gyűjtemény mérete több, mint 3 TB, ami önmagában is tetemes mennyiségű személyes adat, videó és kép, különböző korú és nemű emberekről, különböző helyzetekben. A privát felvételek nemcsak Szingapúr, hanem Kanada, Dél-Korea vagy Thaiföld különböző területeiről származnak. A hackercsapat rafinált módon 700 MB adatot és 4000 képet, videót közölt ingyenes mintaként, így a csábításnak engedő ügyfelek azonnal teljesítették a díjfizetést. A feltört kamerák képét természetesen az ügyfelekkel is megosztották. A helyi informatikai szakemberek véleménye szerint az IP kamerák feltörését a kamerák technikai, vagy az alkalmazott szoftverek sérülékenysége, biztonsági rések, illetve a gyenge felhasználói jelszavak kihasználása segítette elő. Vélhetően a feltört IP kamerával rendelkező felhasználók nagy része nem is tud az incidensről és továbbra is gyanútlanul használja kameráját magáncélokra. Az említett incidens ellenére Szingapúr állam jelentős technikai (építészeti, informatikai) fejlettséggel rendelkezik. Ezt bizonyítja a Szingapúri Kormányzati Ügynökség által meghirdetett Szingapúri Nemzetközi Kiberhét 2020., ahol a régió egyik legnagyobb ötödik információbiztonsági eseményét rendezték meg, több, mint 6000 résztvevővel 60 országból. A Szingapúri Kiberbiztonsági Ügynökség (CSA) szervezésében a SICW 2020-ban 138 előadó vett részt, az ipar képviselői mellett kormányok és akadémiák is képviseltették magukat. Nemcsak Európában, az Amerikai Egyesült Államokban, de távol keleten is fontos kibertér védelme. A CSA nyilatkozata szerint együttműködik a partnerekkel többek között az információbiztonsági tudatosság növelése, az erőteljes munkaerő által támogatott élénk információbiztonsági ökoszisztéma kiépítése, nemzetközi partnerségek kialakítása érdekében.[315] [316] A szingapúri informatikai incidensek 40% -ában a hackerek a munkavállalói adatot célozzák meg, mert így további adatokhoz, vagy illegálisan szerzett bevételhez juthatnak. Természetesen nemcsak a Távol-Kelet dicsekedhet az informatikai incidensek számosságával. Kanadában és az Egyesült Királyságban is jelentősen megnövekedett a hacker

[313] Cyber Security Agency of Singapore, Singapore Cyber Landscape 2018.
[314] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, IT biztonság, Hírek, Több, mint 50 000 otthoni IP kamerát tört fel egy hacker csoport, https://nki.gov.hu/it-biztonsag/hirek/tobb-mint-50-000-otthoni-kamerat-tort-fel-egy-hacker-csoport/, 2020. október 21., letöltés: 2022. augusztus 7.
[315] Singapore Government Agency: Singapore International Cyber Week 2020, https://www.csa.gov.sg/news/press-releases/sicw-2020-highlights-and-testimonials, letöltés: 2020. október 30.
[316] Statista Research Department: Impact of cyber security incidents in Singapore 2016 https://www.statista.com/statistics/787025/singapore-impact-of-cyber-security-incidents-on-firms/, letöltés: 2020. október 30.

tevékenységek száma. A 2017. évi kanadai felmérés alapján az érintett kanadai vállalkozások számának több, mint fele (54%) arról számolt be, hogy az információbiztonsági incidensek megakadályozták az alkalmazottak napi munkáját, és a vállalkozások közel 30 %-a további helyreállítási költségekkel számolt. Kanadában a legnagyobb kárt a banki, kereskedelmi és felsőoktatási szektor szenvedte el, ahol hackerek a működést gátolták, pénzt loptak vagy pedig adataikért váltságdíjat követeltek. A felmérés szerint a kanadai nagy (91%), közepes (83%) és kis (72%) vállalkozások többsége arról számolt be, az alkalmazottai a felelősek vállalkozásuk általános kiberbiztonságáért, ebből egyszerűen következtetve az elszenvedett incidensekért is.[317] A hivatkozott felmérés az információbiztonságiincidensek típusával is foglalkozott. Az információbiztonsági incidensek által érintett vállalkozások 39% -a nem tudta beazonosítani a támadás okát, 38%-a nyilatkozta, hogy a hackerek pénzt lopni vagy váltságdíjat követelni próbáltak vagy esetlegesen meg is tették. A vállalkozások alig több, mint egynegyede (26%) tapasztalt olyan eseményeket, amikor az elkövetők megpróbáltak illetéktelen vagy védett területekre, rendszerekbe bejutni, míg 23% személyes vagy pénzügyi információk megszerzésére irányuló eseményeket tapasztalt.[318] A kanadai vállalkozások többsége (85%) arról számolt be, hogy szerintük a jövőben megnő az információbiztonsági kockázatok és fenyegetések iránti kiszolgáltatottság, ami a rendelkezésre álló adatok alapján is aggodalomra ad okot. A vállalkozások 60%-a jelezte, hogy az adataik illetéktelen kézbe kerülése vagy rosszindulatú manipulálása, 56%-uk szerint a rosszindalatú programok (szoftverek, vírusok, kéretlen reklám, ransomware) és 47%-uk jelezte, hogy a különböző internetes csalás (gazdasági csalás vagy adathalászat) kifejezetten káros hatással lenne az üzleti tevékenységükre. Nemcsak államok, hanem nagyvállalatok is foglalkoznak a számítógépes bűnözés adatainak értékelésével, ami alapján döntenek a kibervédelmi intézkedések szükségességéről. Az Adidas kétmillió rekordnyi adatsérülése, valamint a Facebook kétmilliárd fiókfeltörése, vagy a Morrison munkatársainak adatszivárgással (2014-ben több, mint 100.000 alkalmazott béradatát szivárogtatták ki) kapcsolatos jogi csatája és kártérítési igénye rámutat arra, hogy mind a nagyvállalatok, mind pedig a felhasználók hatalmas adatsérülést vagy –vesztést szenvednek el. 2018. első félévében 4,5 milliárd adatrekord került veszélybe és az incidensek súlyossága 133 %-kal nőtt.[319] A Breach Level Index 2018. évi felmérése (BLI) alapján csaknem 15 milliárd

[317] Howard Bilodeau, Mohammad Lari and Mark Uhrbach, Cyber security and cybercrime challenges of Canadian businesses, The Canadian Centre for Justice Statistics, 2017.
[318] Győrffyné Holló Krisztina, Az információbiztonsági tudatos viselkedés az incidensek elkerülésének egyik tényezője, DUNAKAVICS 8 : 12 pp. 5-18. , 14 p. 2020.
[319] S. Trabelsi, Monitoring Leaked Confidential Data, 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2019, pp. 1-5, doi: 10.1109/NTMS.2019.8763811.

adatrekordot tettek közzé 2013-2018. között és 2013. és 2019. év között 9,7 milliárd adatrekordnyi (identity) eltulajdonítás vagy adatvesztés történt a világban. A 2018. évi felmérés alapján megállapították, hogy az adatlopás csaknem 64%-a az Amerikai Egyesült Államokban történt. Lakosság arányú adatlopás mértékét tekintve a lista élén szintén az Egyesült Államok (19) áll, de ez a mérték jelentős Dél-Koreában (4,5), Kanadában (2,5) és az Egyesült Királyságban (2,1) is. [320]

4.2.1.2. AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEK STATISZTIKAI ADATAI (2019-2021)

Az alábbi fejezetben a GDPR, Infotv. hatályba és életbe lépését követő 2019.2021. időszak kutatásomhoz kapcsolódó információbiztonsági események és statisztikai adatok vizsgálatának eredményét foglalom össze. Ebben az időszakban nemcsak a GDPR alkalmazásának tapasztalatait, hanem a COVID-19 világjárvány hatását, úgymint a munkavállalók otthoni munkavégzéshez szükséges saját eszközhasználatra vonatkozó távmunka szabályait is figyelembe kell venni. Az időszak első felére az új szabályok és lehetőség bevezetése és működtetése (2019-2020. első félév), míg a második felére inkább az ellenőrzés és beavatkozás (2020. második félév – 2021.) a jellemző[321] Az időszak első felét sem kímélték a kibertámadók. 2019. nyarán az ausztrál egyetem megerősítette, hogy a 2018. év végi adatvédelmi incidens becslések szerint 200 000 hallgatót és munkavállalót érintett Az incidens során hozzáfértek az érintettek személyes adataihoz, tehát nevek, címek, születési dátumok, telefonszámok, személyes e-mail címek, sürgősségi elérhetőségek, adószámok, bérszámfejtési adatok, bankszámla adatok, útlevél adatok és hallgatói tanulmányi adatok kerültek veszélybe. Az incidenst hónapokig vizsgálták, de bizonyítékot nem találtak kutatási vagy egyéb személyes adatokhoz való hozzáférésre, adatlopásra.[322] Az időszakra jellemző adatvédelmi jogsértések közé tartozott például a bankkártya adatok hibás szerverkonfiguráció miatti kiszivárogtatása[323], az American Medical Collection Agency adatszivárgása (7,7 millió érintett személy, 11,9 rekord)[324] vagy a Zynga mobiljáték-gyártó ügyfél adatainak szivárgása (218 millió iOS és

[320] Győrffyné Holló Krisztina, Információbiztonság avagy megéri kockáztatni?, Az informatika korszerű technikái konferencia 2020, Jövőformáló tudomány, Tudományos HÉT 2020, Dunaújvárosi Egyetem

[321] COUNCIL OF THE EUROPEAN UNION, COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020, amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN, letöltés: 2022. február 26.

[322] Australian National University, ANU releases detailed account of data breach (2019.)

[323] Bankkártya adatokat szivárogtatott egy kanadai mobil szolgáltató, Nemzeti Kibervédelmi Intézet, 2019. https://nki.gov.hu/it-biztonsag/hirek/bankkartya-adatokat-szivarogtatott-egy-kanadai-mobil-szolgaltato/, letöltés: 2022. február 26.

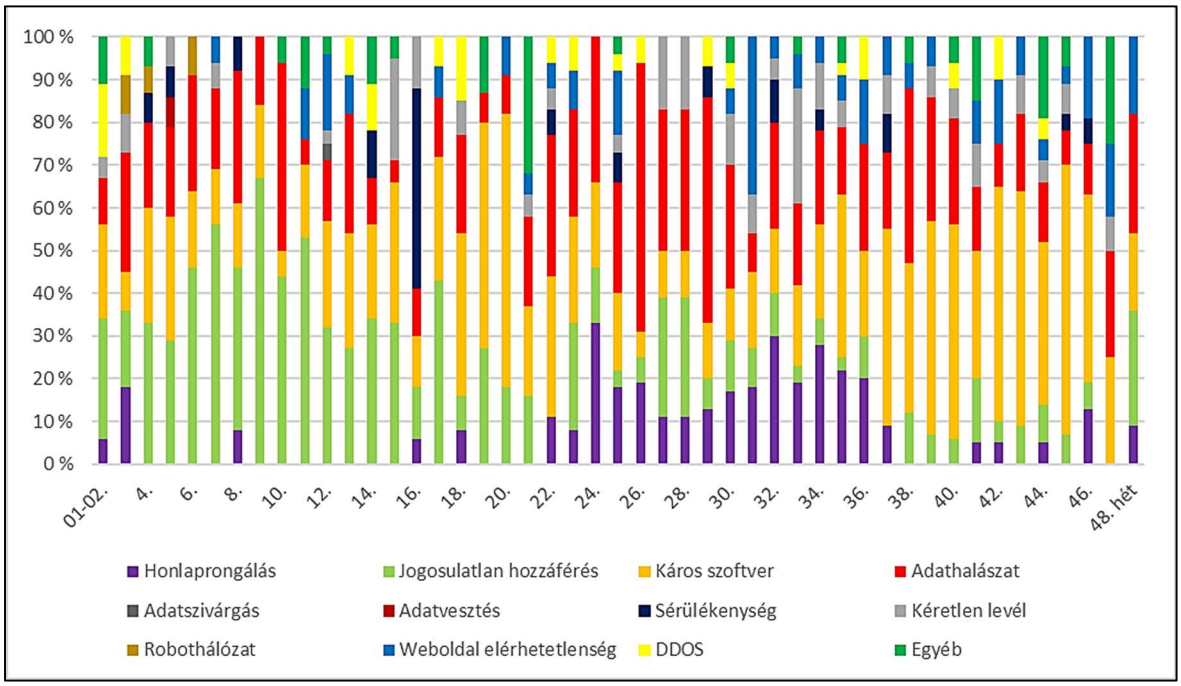
[324] AG Shapiro Announces Multistate Settlement With American Medical Collection Agency Over 2019 Data Breach, Pennsylvania Office of Attorney General, 2021., letöltés: 2022. február 26.

Android ügyfél bejelentkezési és Facebook azonosítója, telefonszáma, e-mail címe) [325].[326] Az időszak második felében az ENISA jelentése (ENISA Threat Landscape - ETL) szerint tovább nőtt az információbiztonsági támadások száma, a COVID-19 világjárvány következtében a „home office", a hibrid irodai modell növelte a támadási felületet[327] és nehezítette a kibervédelmi szakemberek segítségnyújtását. A jelenléti irodai tevékenységek átállása online térbe, valamint a növekvő felhőmegoldások alkalmazása a kiberbűnözőkre ösztönző hatással van, ugyanakkor az újdonságok, az összekapcsolhatóság (informatikai interoperabilitás), a mesterséges intelligencia (MI) technológiái bővítik és erősítik az információbiztonsági környezetet és a kibervédelmi szakemberek egyre több információval rendelkeznek a támadások kifinomultságáról, összetettségéről és hatásáról (Network and Information Security Directive - NISD). Az információs rendszereink az MI által is taníthatók. Incidensek tekintetében 2020-2021. években kiemelt információnak számít a Norvég Parlament, az új-zélandi tőzsde, a német Választási Hatóság, a belga kormányzati webes szolgáltatások, valamint az ausztrál kormányzati szervek ellen indított kibertámadás, de nem kímélte a zsarolóvírus a brit oktatást, az argentin határátkelőhelyeket, az ír egészségügyet, az új-zélandi kórházakat vagy az Acert. Adatszivárgás vagy adatlopást jelentettek a T-Mobile, LinkedIn, illetve a Shell szakemberei. Az incidensekről és a kibervédelmi útmutatókról, tanácsokról[328] heti szintű rendszerességgel tájékozódhatunk az NBSZ NKI publikus honlapján és közösségi oldalán. Az intézkedési igények szükségességét informatikai szakemberek által összegyűjtött incidens adatok is alátámasztják, amely szerint 2021-ben volt a legmagasabb átlagos költség az elmúlt 17 évben. Az adatszivárgás költségei 3,86 millió USD-ról 4,24 millió USD-ra emelkedtek, ami a legmagasabb átlagos összköltség az elmúlt 17 évben.[329] A biztonsági események nagyságrendje, gyakorisága és hatása évről évre, exponenciális mértékben növekszik. A kiberbűnözés elleni válaszreakció szükségességét erősítve az Európai Tanács 2020. július 30-án úgy határozott, hogy korlátozó intézkedéseket vezet be hat személlyel és három szervezettel szemben, akik különféle kibertámadásokért felelősek vagy részt vettek a bűncselekményben (OPCW - Organisation for the Prohibition of Chemical Weapons elleni

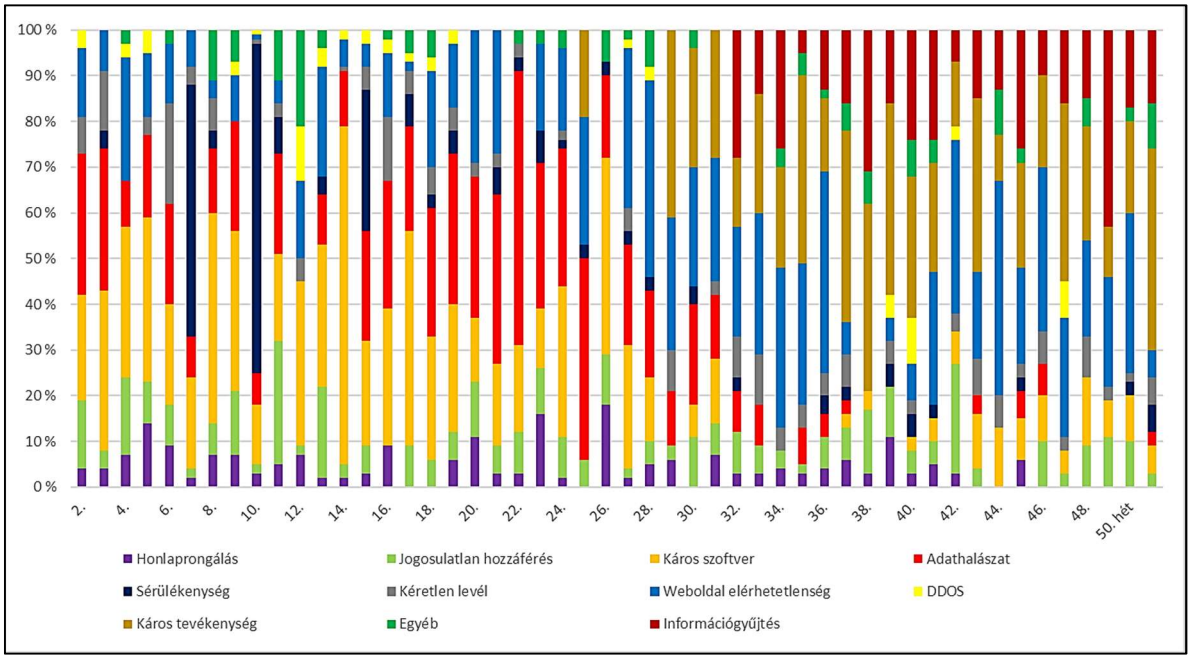
[325] R. T. Kamurthi, S. R. Chopra and R. Sharma, Confrontation-Wi-Fi Risks and Data Breach, 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), 2021, pp. 633-638, doi: 10.1109/ESCI50559.2021.9397047.
[326] Wagner, Paul, Third Party Breaches - A Survey of Threats and Recommendations, United States, 2021. SSRN http://dx.doi.org/10.2139/ssrn.3782822, letöltés: 2022. február 26.
[327] ENISA Threat Landscape 2021.
[328] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, IT-biztonsági tanácsok, https://nki.gov.hu/it-biztonsag/tanacsok/, letöltés: 2022. augusztus 7.
[329] IBM, Ponemon Institute, Cost of Data Breach Study, 2021.

kibertámadási kísérlet, „WannaCry", „NotPetya" és „Operation Cloud Hopper" néven ismert kibertámadás). A kiszabott szankciók között szerepel az utazási tilalom (az érintett személyek nem utazhatnak be az EU területére) és a vagyoni eszközök befagyasztása. Továbbá az EU-beli személyeknek és szervezeteknek tilos pénzeszközöket rendelkezésre bocsátani a kiberbűnözők, hackercsoportok számára. A szankciók az EU kiberdiplomáciai eszköztárában rendelkezésre álló lehetőségek egyike az EU vagy tagállamai ellen irányuló rosszindulatú kibertevékenységek megelőzésére, elrettentésére és válaszreakcióra. Ez volt az első olyan alkalom, amikor az EU szankciókat fogalmazott meg a kibertámadásért felelős bűnözők számára, tehát ez a lépés mérföldkő az EU-t és tagországait ért hackeltámadásra adott válasz tekintetében.[330] Az NBSZ NKI által közzétett 2021. évi 49. számú Nemzetközi IT-biztonsági sajtószemle[331] incidens adatai vizsgálata szerint 2021.12.03. és 2021.12.09. közötti, karácsony előtti időszakot tekintve az incidensek eloszlása kockázati besorolás szerint 95%-a alacsony és 5%-a közepes mértékű, továbbá az incidenstípusok eloszlása szerint 4%-a honlaprongálás, 4%-a jogosulatlan hozzáférés, 14%-a káros szoftver, 14%-a weboldal elérhetetlenség, 23%-a egyéb és 41%-a adathalászat volt. A NBSZ NKI által közzétett adatok alapján megállapítottam, hogy míg 2017-ben a karácsony előtti időszakban a legelterjedtebb incidenstípus a káros szoftver (82%) volt, 2021-ben pedig az adathalászat (41%). A támadástípusok 2019-2021. év heti eloszlását a következő grafikonok szemléltetik. A vizsgálat során megállapítottam, hogy a hazai statisztikai adatok is megerősítik azt a tényt, miszerint a legelterjedtebb támadástípus 2019. és 2020. első félév között a káros szoftver a jogosulatlan hozzáférés és az adathalászat volt, míg 2020. második felében a weboldal elérhetetlenség, a káros tevékenység és az adatvesztés, valamint 2021. évben az adathalászat, a weboldal elérhetetlenség, a káros szoftver és az egyéb besorolású incidenstípus. (9., 10., 11. ábra)

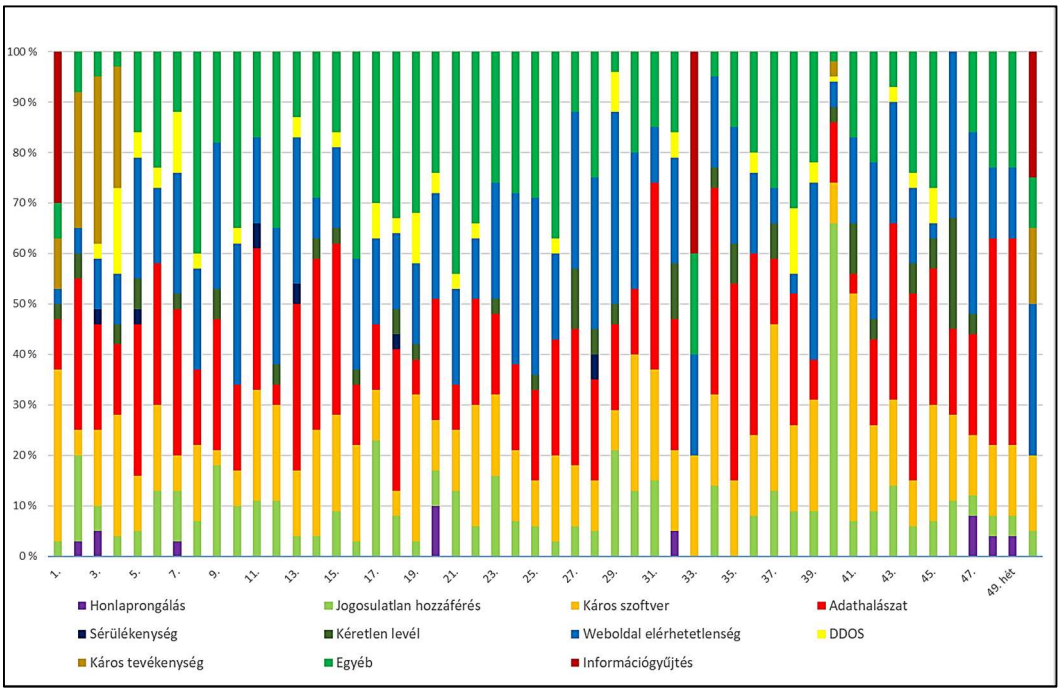
[330] European Council, EU imposes the first ever sanctions against cyber-attacks (2020.)
[331] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, IT-biztonsági sajtószemle, https://nki.gov.hu/it-biztonsag/kiadvanyok/sajtoszemle/, letöltés: 2022. augusztus 7.



9. ábra, Incidenstípusok eloszlása NBSZ NKI statisztikai adatai alapján – 2019. 1-48. hét saját adatgyűjtés, vizsgálat alapján saját szerkesztés

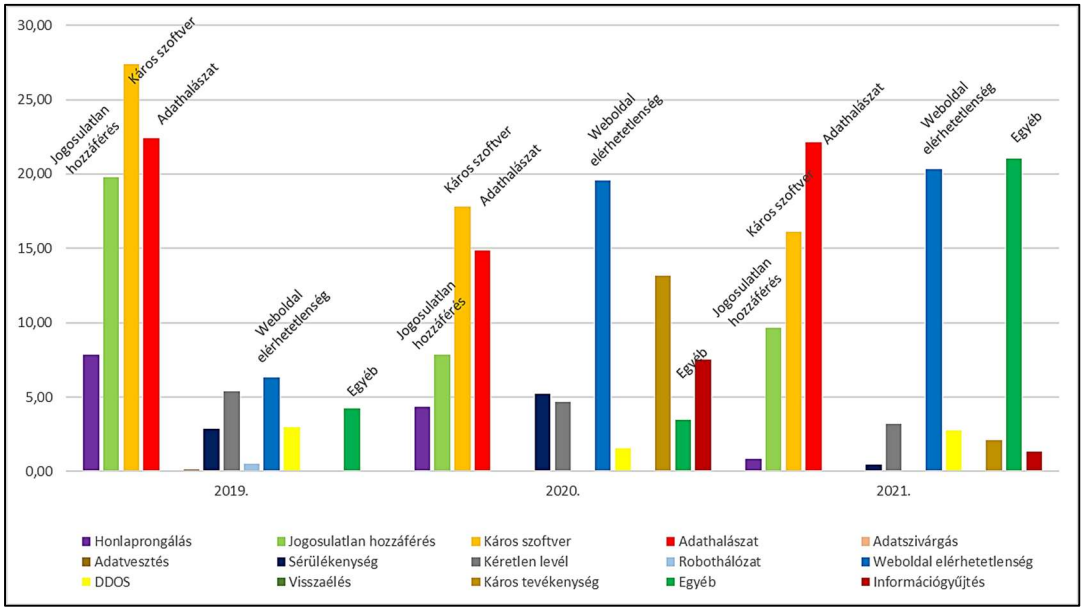


10. ábra, Incidenstípusok eloszlása NBSZ NKI statisztikai adatai alapján – 2020. 1-51. hét saját adatgyűjtés, vizsgálat alapján saját szerkesztés



11. ábra, Incidenstípusok eloszlása NBSZ NKI statisztikai adatai alapján – 2021. 1-50. hét saját adatgyűjtés, vizsgálat alapján saját szerkesztés

Az elmúlt három évet tekintve megállapítható, hogy a káros szoftver (átlag 20,44%), az adathalászat (átlag 19,80%) és a weboldal elérhetetlenség (átlag 15,40%), valamint a jogosulatlan hozzáférés (átlag 12,43%) volt a legkedveltebb kiberbűnözői tevékenység. (12. ábra).



12. ábra, Incidenstípusok eloszlása NBSZ NKI statisztikai adatai alapján – 2019-2021. saját adatgyűjtés, vizsgálat alapján saját szerkesztés

4.2.1.3. AZ INFORMÁCIÓBIZTONSÁGI SEBEZHETŐSÉGEK ÉS FENYEGETÉSEK LEHETSÉGES KATEGÓRIÁI

A rosszindulatú fenyegetések (malware) kategóriáit meglehetősen nehéz összeállítani, mivel folyamatosan új rosszindulatú programok születnek és a mintegy napi 360 000 új kártevő statisztikája ijesztőnek tűnik, ugyanakkor ezek közül az „új" kártevők közül sok a régebbi rosszindulatú programok átalakítása, amelyeken sokszor csak annyira módosítottak, hogy felismerhetetlenné tegyék őket a víruskereső programok számára. Az évek során azonban sokféle rosszindulatú program jött létre, amelyek mindegyike más módon befolyásolja a célrendszert vagy programot. Például a Ransomware nevű rosszindulatú szoftvert arra tervezték, hogy titkositsa az áldozat adattároló meghajtóit, így a tulajdonos hozzáférését meggátolja. A feloldásért, a titkosítási kulcsért cserébe általában pénzt követelnek. Amennyiben a váltságdíjat nem teljesítik, a kulcs törlődik, és az adatok örökre elvesznek vele. Közkedvelt a trójai program is, ami lényegét tekintve minden olyan rosszindulatú program, amely legitim programként álcázza magát annak érdekében, hogy feltelepítsék a rendszerbe. A trójai sok kárt okozhatnak, mert a biztonsági védelem mögé kerülnek, és komoly veszélyt hordoznak magukban, csakúgy, mint az a bizonyos hírhedt ló Trója városában, Homérosz „Iliászában". A férgek olyan programok, amelyek önállóan képesek lemásolni és elterjedni különféle eszközökkel, például e-mailek segítségével. Miután a rendszerbe került, a féreg megkeresi a kapcsolattartók adatbázisának vagy fájlmegosztó rendszerének valamilyen formáját, és mellékletként is elküldheti magát. A férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. Számos rosszindulatú program célja, a bizalmas adat elérése, másolása, átírása vagy törlése. Néhány magas fejlettségű kártevő program önállóan lemásolhatja az adatokat, és elküldheti azokat egy adott szervernek, további felhasználásra. Az alapvető víruskereső védelmet nyújthat egyes rosszindulatú programok ellen, de az optimális védelem biztosításához többrétegű biztonsági megoldás szükséges, amely víruskeresőt, mélycsomag-ellenőrző tűzfal ellenőrzést, behatolás-észlelő rendszer használatát, e-mail víruskeresőt és munkavállalói tudatosságnövelő képzést foglalja magába. Az értekezésnek nem témája a különböző rosszindulatú programok bemutatása és elemzése, ugyanakkor ezek közül, a témához kapcsolódó néhány példa megemlítése elengedhetetlen. A sérülékenységek, a biztonsági rések is komoly kockázatot jelentenek, és támadási felületet biztosítanak a hackereknek. Naponta számtalan új fenyegetést fejlesztenek ki, és ezek általában az ismert vagy kevésbé ismert biztonsági réseket használják ki. Egy-egy fejlesztés során több, le nem tesztelt biztonsági rés keletkezhet. A fejlesztői tesztelések során ezekre a sebezhetőségekre jórészt fény derül, és sikerül kijavítani. Egy-egy új szoftververzió megjelenését gyakran követi a biztonsági

csomag is, amelynek mielőbbi telepítését a gyártók is javasolják. Az elmaradt biztonsági szoftverfrissítés következménye lehet az incidens, tehát a támadók a biztonsági réseken keresztül is okozhatnak kárt. Biztonsági rés lehet egy nyitva hagyott csatorna, nyílt hozzáférés egy ügyfél adatbázishoz is. Véleményem szerint a biztonsági frissítés idejét nehéz optimálisan megválasztani, hiszen a frissítés idejére a számítógépet vagy a szervert, illetve az alkalmazásokat nem használhatjuk, ezért egyes esetekben kellemetlenséget okoz, viszont pénzkímélő és adatvesztéssel járó bosszúságot takaríthatunk meg. A megoldás a kellemetlen helyzetek elkerülésére a biztonsági frissítések ütemezése, lehetőleg ugyan azon napon, napszakban, ezáltal kiszámíthatóbb tevékenységgé tehetjük és a felhasználók is figyelembe veszik munkájuk és szórakozási tevékenységük során. A rendszertelen frissítések következménye a tevékenységre vonatkozó átláthatatlan, kiszámíthatatlan és bosszantó vélemény kialakulása, ami információbiztonsági szempontból a rendelkezésre állás elvét befolyásolja. A rejtett hátsó ajtó lényegénben egy szándékosan létrehozott számítógépes biztonsági rés, amely esetben a gyártó által telepített program úgy van kialakítva, hogy lehetővé tegye a számítógép, rendszer vagy program távoli elérését, hozzáférését. A szoftveres sebezhetőségek egyik kiemelt problémája a rendszergazdai jogosultságok nem megfelelő kezelése. Minél kevesebb információhoz vagy erőforráshoz fér hozzá a felhasználó, annál kevesebb kárt okozhat. Számos szervezet nem tudja megfelelően ellenőrizni a felhasználói fiókokhoz való hozzáférési jogosultságokat, ami lehetővé teszi az úgynevezett „Superuser” vagy rendszergazda szintű hozzáférést olyan felhasználók számára is, akik beosztásuknál vagy képzettségüknél fogva kevésbé jogosultak rá. A számítógépes biztonsági rések kezelése szempontjából elengedhetetlen a jogosult felhasználók információbiztonsági hozzáférés ellenőrzése. A hozzáférések kezelését naplózni szükséges. Parancsfájlok automatikus futtatása kártékony programok és vírusellenőrzések nélkül, ez az egyik általános hálózati biztonsági rés, amelyet egyes hackerek megtanultak kihasználni bizonyos webböngészőket „megbízható” vagy „biztonságos” szkriptek automatikus futtatására. Ezáltal a kiberbűnözők elérhetik a böngésző szoftverét, és rosszindulatú programokat futtatnak gyakran a felhasználó tudta nélkül.

Biztonsági hibák (Security Bugs) a program vagy adatbázis-interfészben. Két vagy több alkalmazás összekapcsolódása esetén az alkalmazások együttműködési nehézségei által programozási problémák és konfliktusok lehetnek, amelyek biztonsági réseket szoftveres sebezhetőséget okozhatnak. Adathalász (Social Engineering) támadás során a támadó megpróbálja becsapni az áldozatát, a vállalat vagy intézmény egyik alkalmazottját, annak érdekében, hogy részére kiadjon személyes vagy jogosultsági adatokat, vagy rosszindulatú

programokat telepítsen. A támadás leggyakoribb formája az adathalász e-mail, amely a szervezet egyik partnerének nevében kér hitelesítő vagy személyes adatokat. Az becsapós e-mailek nyelvezete rendszerint hibás és a hivatkozott link nem a partner ismert weboldalára mutat. Számos módja létezik az adathalász támadási stratégia ellen védekezésnek, különösen az e-mail víruskereső eszközök, szoftverek, vagy a többtényezős hitelesítés (MFA - Multi-factor authentication) alkalmazása. További védekezési lehetőséget nyújtanak az alkalmazottak információbiztonsági tudatosság képességének fejlesztése következtében alkalmazott eljárások. Kutatásom során tapasztaltam, hogy egy képzett munkavállaló kevésbé esik az adathalász csapdájába, mint az, aki nem ismeri az alapvető információbiztonsági protokollokat. Az információbiztonsági képességeket fejlesztő tréning segíti az alkalmazottakat az alapvető, az adathalász támadások azonosításához és elkerüléséhez szükséges ismeretek megszerzésében. További lehetőség a mélyreható védelmi intézkedések alkalmazása. A többszintű hálózatbiztonsági védelem használata során, ha a támadó megkerüli a hálózat külső védelmét, akkor a további védelmi rétegek nehezítik a továbbjutást és a védett eszköz megközelítését. A korlátozott felhasználói hozzáférés (Policy of Least Privilege), amely szerint korlátozzuk a felhasználói hozzáférését, a munkaköri feladatok ellátásához szükséges hozzáférések számát. Ily módon, ha visszaélnek a felhasználói hozzáféréssel, jogosultsággal, akkor az okozott kár kisebb lesz. Az IoT-eszközök sebezhetősége abban rejlik, hogy okos eszközeinkkel immár tv-t, wifi eszközt, nyomtatót, takarítórobotot, hűtőszekrényt vagy kávéfőzőt is vezérelhetünk, de ezeket az okos eszközök más alkalmazások, „*app*”-ok számára is elérhetővé válnak, ezáltal hozzáférhetnek nemcsak a személyes adatokhoz, kapcsolatokhoz, képekhez, videókhoz, hanem átvehetik az irányítást az eszköz felett. A hálózaton keresztül pedig más okos eszközt is elérhetnek. A rendszeres eszközellenőrzés elengedhetetlen, mivel sokszor ezeket a műveleteket a tulajdonos észre sem veszi.

4.2.2. AZ INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER

Az alábbi fejezetben bemutatott ISO/IEC 27001 szabvány alapú információbiztonsági irányítási rendszer (ISMS) [332] előírások szerinti bevezetése és működtetése biztosítja az információs rendszer fenntarthatóságát és fejleszthetőségét egyben az információbiztonsági követelményeknek való megfelelést. Kutatásom elengedhetetlen részét képezte az ISMS

[332] Information Security Management System, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001 szabvány - Információbiztonsági Irányítási Rendszer, https://www.iso.org/isoiec-27001-information-security.html, letöltés: 2021. április 24.

bevezetése és működtetése, ennek keretében pedig a releváns kockázatkezelési módszerek kutatása és felhasználása az információbiztonsági kockázatok csökkentése érdekében, valamint további statisztikai adatgyűjtéshez és kiértékeléshez. Az előbbiek értelmében indokolt az ISMS bevezetésének és működtetésének bemutatása, a kockázatkezelési módszerek és azok felhasználhatóságának ismertetése, amely a kutatásom incidensek vizsgálatának részéhez kapcsolódik. Az Információbiztonsági irányítási rendszert olyan szervezetek (vállalatok, intézmények) vezetik be és használják, amelyek az Infotv. és az ISO/IEC 27000 szabványcsalád, Információbiztonsági Irányítási Rendszer szabványa alapján működtetik szervezetüket és az általuk nyújtott szolgáltatás vagy termék előállítása és értékesítése szempontjából jelentős szerepet kapott az ISMS szabályainak alkalmazása. A szabvány alkalmazása és az ISMS bevezetése, valamint működtetése nem zárja ki az Uniós rendelkezések, hazai jogszabályok szervezeten belül szabályozási rendszerben való rögzítését, sőt az ISMS bevezetése és a szervezet szabályainak rendszerbe foglalása támogatja az irányítási, munkaügyi, adatvédelmi, információbiztonsági és informatikai előírások rögzítését, valamint elősegíti a stratégiai, kockázatkezelési, üzletmenetfolytonossági és intézkedési előírások gyakorlati megvalósítását. A bevezető részben említett Balanced Scorecard módszer alkalmazása hozzájárul az átlátható intézkedési tervek megvalósításához. Sajnálatos módon jelen dokumentum terjedelme nem engedi meg, hogy teljes fejezetet szánjak e jelentős módszer felhasználásának (stratégiai térkép) bemutatására. A módszer előnye, hogy az intézkedési terv folyamatai átláthatóbbak, a bemeneti adatok, a csomópontok és „forgalomirányítók”, az ok-okozati összefüggések, valamint a kiindulási állapot és a célkitűzések. Az intézkedési terv egyik lényeges tényezője, hogy a kockázatok mértékét a lehető legkisebbre csökkentsük. Bár ez nem kifejezetten gazdasági terv, de alkalmazásának hatékonysága közvetett módon hat a szervezet pénzügyi helyzetére, ezért a Balanced Scorecard módszer elvei alkalmazhatóak. Az információbiztonsági irányítási rendszer meghatározó részét képezi a kockázatmenedzsment, a kockázatkezelés, benne a vagyonelemek felmérésével, a fenyegetések és sebezhetőségek értékelésével és az intézkedési terv alkalmazásának szervezetre való hatásával. Az ISMS fontos részét képezi az információbiztonsági politika, amely rögzíti a biztonság iránti elkötelezettséget, és az információbiztonsági célokat. Kidolgozásánál a második fejezetben már ismertetett elvek figyelembe vétele elengedhetetlen. A szervezet az információbiztonsági politikában meghatározhatja az alábbi iránymutatásokat és elveket, így például az információbiztonsági politika kiterjedését és célját, az információbiztonság meghatározását, általános célkitűzéseit és tárgykörét, valamint a biztonság fontosságát, a vezetőség

szándéknyilatkozatát, amely támogatja az információbiztonság céljait és elveit, az információbiztonság „*szervezési elveit, ide értve a szervezeti struktúrát, a személyi felelősségeket és hatásköröket, a szervezet tulajdonában levő adatvagyon elemeinek érzékenységét, az ennek megfelelő védelmi szinteket, és a biztonsági osztályozási rendszert, továbbá – ha van ilyen – az osztályba sorolástól eltérő védelmi igényű adatkörök védelmére vonatkozó politikát, a kockázatok felmérésére és kezelésére vonatkozó elveket, a belső személyzettel és a külső partnerekkel kapcsolatos biztonságpolitikát*", az információbiztonsági ellenőrzés rendszerét (IT Audit), az „*információbiztonsági feladatok megosztására vonatkozó elveket*", valamint „*a biztonságpolitika változásának ellenőrzési eljárását és felülvizsgálatának körülményeit*". Az információbiztonsági politika keretet ad az ISMS szabályozási rendszernek, lényegét tekintve összefoglaló szerepe van. Az irányítási rendszerek egyik jelentős modellje a PDCA a modern típusú menedzsment kulcseleme. A legtöbb szervezet nem zárkózik el a fejlődés elől, de a meghatározott és szükséges változtatásokat sok esetben a régi típusú adminisztrációs folyamat vagy megszokott szervezeti működés is gátolhatja az előrehaladást és megállíthatja az innovációt. A Plan-Do-Check-Act modell,[333] amely egy iteratív módszer a folyamatok, termékek vagy szolgáltatások folyamatos fejlesztésére és amely szerint elvégzett tevékenységsorozat segít kiszakítani a szervezetet a stagnálás állapotából és áttérni a folyamatos fejlesztés rendszerére. A PDCA modell előnyeit az információbiztonsági irányítási rendszer is használja és szinte azonnal tapasztalhatók a régi és az új szervezeti működés közti különbségek. A PDCA modellt az 1950-es években Dr. W. Edwards Deming fejlesztette ki, mint a problémamegoldás tudományos módszerén alapuló tanulási vagy fejlesztési folyamatot. Az PDCA modell az ISMS tervezésére vagy létrehozására, bevezetésére és működtetésére (végrehajtás), ellenőrzésére, valamint továbbfejlesztésére és beavatkozására fejlesztett modell. Minden állomásában újabb PDCA modell szerinti folyamatábra alakítható ki. Az „*első szakasz a Tervezés (Plan) – a fennálló helyzet tanulmányozása, adatgyűjtés, javítás megtervezése, a második szakasz a Végrehajtás (Do) – a terv kipróbálása kísérleti jelleggel egy kisebb projekt vagy a felhasználók egy szűkebb körén belül alkalmazva, a harmadik szakasz az Ellenőrzés (Check) – a változtatások hatásának elemzése és értékelése, és a negyedik szakasz a Beavatkozás (Act) – a bevált módszer bevezetése*" és szabványosítása[334]

[333] Muha Lajos, Szádeczky Tamás, Irányítási rendszerek, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, 2014.
[334] Muha Lajos (szerk.): Az informatikai biztonság kézikönyve, Verlag Dashöfer, Budapest, 2000-2005

4.2.2.1. AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATMENEDZSMENT

A kockázatmenedzsment elengedhetetlen része az időszakos helyzetfelmérés és -értékelés, amelyek között különösen megemlítendő az egyes speciális kutatási módszerek, úgymint a „*Social Engineering"* információszerzési módszerek (kérdőívek, megfigyelések, adatbányászat alkalmazása), a felhasználói közreműködést igénylő fenyegetés- és támadásvizsgálatokra irányuló információszerzési módszerek (megfigyelési és mintavételezési eljárások), kockázatelemzési módszerek, (mintavételezési, kvalitatív és kvantitatív módszerek) alkalmazása. A szervezetek kockázatkezelése mindig egyedi, mivel a különböző tevékenységeket végző szervezeteknek különböző típusú kockázattal, azok elemzésével és kezelésével kell szembenézniük. A szervezetek egyedi információbiztonsági kockázati profillal rendelkeznek. A kockázatkezelés lehet gazdasági, ipari vagy informatikai jellegű, amelyet mindig a szervezet célmeghatározása és politikája dönt el. A fejlődés adta lehetőség, hogy immár önálló területté nőtte ki magát mind a szervezetekben, mind a tudományos kutatásban és az oktatásban, amely szakosodott tudást, készségeket igényel. Az IT eszközök széles körű elterjedése és dinamikus fejlődése jelentősen befolyásolja az IT kockázatmenedzsment összetevőit, így a vagyonelem detektálást és elemzést, helyzetfelmérést, kockázat típusmeghatározást, a vagyonelemekre vonatkozó kockázatelemzést, kockázatkezelést és intézkedéseket valamint eredménykimutatásokat. Az ISMS bevezetésével a helyzetfelmérés elengedhetetlen, amelyek elvégzése a következő területekre nézve különösen fontos: a szabályozási környezet, a szervezeti biztonság, a vagyontárgyak biztonsága, az emberi erőforrások biztonsága, a fizikai és környezeti biztonság, a kommunikáció és üzemeltetés biztonsága, a hozzáférés-ellenőrzés, a fejlesztés, beszerzés, és karbantartás, az incidenskezelés, a működés folytonosságának irányítása, valamint a megfelelés a jogszabályi környezettel. A kockázatmenedzsment feladatkörébe tartozik az adott információs rendszer sérülékenységének vizsgálata a potenciális fenyegetések és lehetséges incidensek felmérése, a felmérésből származó védelmi stratégia, intézkedések kidolgozása és alkalmazása. Fokozott figyelmet kíván a gyenge láncszem felderítése és kezelése, amelynek nemcsak rendszer, de humán vonatkozásai is lehetnek. Minden kockázati tényező egyedi, éppen ezért egyedi megoldásokat kíván. Az alapvető igény, hogy teljes mértékű védelmi szintet biztosítsunk lehetetlen, de ez nem jeleni azt, hogy nem kell törekedni az elérhető, lehető legmagasabb védelmi szint létrehozására. Ehhez nyújt segítséget a kockázatelemzés és a lehetséges veszteségek pontos ismerete. A vezetőség elé tárt valószínűsíthető, illetve bekövetkezhető veszteségek pénzügyi vonzata elősegíti a tényeken alapuló optimális döntéshozatalt. Bár az informatika világában

meglehetősen nehéz feladat a veszteséges folyamatokat és a lehetséges eszmei és eszközöket ért károkat költséggel ellátni, a helyreállítás során a piac által meghatározott lehetséges költségeket figyelembe kell venni. A védelemre fordított energia és tőkebefektetés lehetőleg ne haladja meg a becsült kár által eredményezett anyagi veszteséget. A kockázatmenedzsment által támogatott, és a vezetés által megfogalmazott, helyes stratégiai döntések és magas szintű szaktudással rendelkező szakemberek együttműködése hozzájárul a hatékony kockázatkezeléshez. A kockázatkezelést ma már komplex kockázatbecslési, kockázatkezelési és szimulációs stratégiák, alkalmazások és módszerek (CRAMM, CISA, COBIT) segítik, amelyek megkönnyítik az optimális intézkedési és védelmi tervek kidolgozását és a vezetői döntést is. A kockázatkezelési terv kidolgozásához jelentős útmutatóul szolgál az ISO/IEC 31000-es szabvány, amely olyan információval rendelkezik, ami hozzájárul egy, a szervezet és a külvilág számára is elfogadható információbiztonsági irányítási rendszer létrehozásához. Hiszen ebben az esetben egy jó kockázatkezelési terven is múlik a felépített rendszer működőképessége, így kutatási eredményeim szerint a terv értéket teremt és védi a szervezetet, a szervezet folyamatainak szerves része, a döntéshozatal segédeszköze, elősegíti a tényeken alapuló döntéshozatalt és kiküszöböli a bizonytalanságot, a rendszeres, ismétlődő, strukturált és aktualitásokat tartalmaz, ugyanakkor szubjektív és nem lehet teljes körű, de szervezetre szabott és egyedi, a szervezeti, emberi és környezeti tényezők figyelembe vétele jelentős, könnyen áttekinthető, az érintettek bevonásával készül, továbbá dinamikus, iteratív, érzékeny a változásokra, és fejlődést elősegítő. Kutatásom során megállapítottam, hogy az informatikai kockázatelemzés nem védelmi intézkedés, elvégzése önmagában nem erősíti a védelmet, de segítséget nyújt ahhoz, hogy létrejöhessen egy biztonságos informatikai rendszer. A kockázatelemzés során számba kell venni a potenciális sebezhetőségeket és fenyegetéstípusokat. Fenyegetések szempontjából lehetnek: külső és belső fenyegetések. Külső fenyegetések (*External Threats*) tekintetében a támadónak nincs hozzáférése a rendszerhez, annak belső erőforrásaihoz (hálózat, szerver, végpontok) és csak a kívülről publikusan elérhető információkat, szolgáltatásokat látja. A sérülékenységet kihasználva hozzáfér a belső erőforrásokhoz. Belső fenyegetések (*Internal Threats*) esetében a támadó hozzáfér bizonyos belső erőforrásokhoz, általában egy felhasználói fiókhoz (gyenge jelszó vagy adathalászat következtében), a belső hálózathoz vagy csupán a biztonsági eljárások gyakorlatához. A támadó célja a jogosultságának kiterjesztése (*Privilage Escalation*), az egyedi, magas szintű jogosultság megszerzése. Fenyegetések típusai lehetnek technológiai eredetűek (fizikai hatás: ipari jellegű, környezetszennyezés), természeti jelenség (árvíz, földrengés, havazás) szerint

klimatikus vagy légköri eredetű (éghajlati - túlmelegedés, szélvihar, klímaváltozás, légköri – villám), illetve geológiai (szeizmikus, vulkanikus, földcsuszamlás, Föld mágneses terének befolyása), továbbá emberi eredetű (szándékos vagy véletlenszerű), úgymint szabotázs, terrorcselekmény. A kockázatfelmérés és a lehetséges gyengeségek és fenyegetések fontosság elismerésének egyik példája, hogy ma már a civil szervezetek, kisebb és nagyobb cégek is próbálnak lépést tartani az elektronikus világ okozta kockázati környezettel, amit jól szemléltet az a tény, hogy 2014-2015. időszakban többet fordítottak információbiztonsági projektekre, mint a megelőző években. A felmérésben részt vevő cégek átlagosan 24 százalékkal növelték információbiztonsági kiadásaikat 2015 évben.[335] A cégek bevallása szerint az információbiztonságra fordított költségek hatására az IT incidensek pénzügyi kára 2014 és 2015 év között 2,7 millió dollárról 2,5 millió dollárra csökkent. A cégek 91 százaléka vezetett be kockázatalapú információbiztonsági irányítási rendszert, és 59 százaléka vásárolt kiberbiztonsági szolgáltatást. Európán belül, az országok kormányai is jelentős összegeket fordítanak kockázatkezelésre és kibervédelemre, ezt a megállapítást támasztja alá Sir Michael Fallon, brit védelmi miniszter nyilatkozata is, amely szerint London milliárdokat költ kibervédelemre.[336] Kockázatkezelés szempontjából az utóbbi időben előtérbe kerülő biometrikus adat tárolása és felhasználása jelentős. Semmi sem eredményezi az innovációt jobban, mint a válság. A megállapítást biometrikus adatokat gyűjtő, tároló és kezelő információs rendszerek dinamikus fejlődése és elterjedése igazolja. A biometrikus módszereket több, mint száz éve használjuk, többek között a bűnüldözési eljárásokban. 1901-ben Angliában és Írországban használtak először ujjlenyomatot a bűnügyi nyilvántartásokban, később 1903-ban az Amerikai Egyesült Államok, New York Állami Börtönében bevezették az ujjlenyomat alapú azonosítást. Nagy fejlődést jelentett az FBI[337] ujjlenyomatok feldolgozására létrehozott részlege 1924-ben, amely 1946-ban már közel 100 millió ujjlenyomattal rendelkezett. 1936-ban pedig Frank Burch lefektette az íriszvizsgálat alapjait. 1960-as évektől számíthatjuk az arcfelismerő berendezéseket, mivel Bledsoe, Goldstein és Lesk munkássága alapján megszülettek az első gépi arcfelismeréssel kapcsolatos eredmények. Ugyanakkor azt is el kell mondani, hogy a biometrikus módszerek elterjedésének korai szakaszában a pontos

[335] Ötvös Gergő, Kiberbiztosítási trendek, Biztosítás és Kockázat, III. évfolyam 1. szám, 2016.

[336] Milliárdokat költenek védelemre, mégis simán kijátsszák őket!, http://www.biztositasiszemle.hu/cikk/nemzetkozihirek/eu/milliardokat_koltenek_vedelemre_megis_siman_kijatsszak_oket.6582.html, letöltés: 2022. február 26.
„*a brit kormány az alig több mint egy éve elvégzett átfogó biztonsági felülvizsgálat keretében a kibertámadásokat hivatalosan a nemzetbiztonságot fenyegető legnagyobb veszélyforrások közé sorolta, és 1,9 milliárd fontot (700 milliárd forintot) különített el az ilyen támadások elleni védelem megerősítésére*."

[337] Federal Bureau of Investigation

meghatározás alulmaradt a vártnál, nagy volt a hibalehetőség is. 1965-ben létrejött az első automatikus aláírás-ellenőrző rendszer, de csak az 1977-es szabadalmazás követően fejlesztették tovább. 1974-ben megjelent az első kereskedelmi forgalomba állított kéz-geometria olvasó, és 1976-ban kifejlesztik a hangalapú azonosítás rendszerét. Később, 1998-ban bevezetésre kerül a DNS-alapú azonosítás és 1994-ben magyar fejlesztés alapján megalkotják az első tenyérlenyomatot használó rendszert. Arcfelismerő rendszert 2001-ben telepítenek először az Egyesült Államokban, egy stadionban, majd a 2001. szeptember 11. után az amerikai hatóságok az összes reptérre biometrikus rendszert vezetnek be.[338] A biometrikus módszerek kifejlesztése és alkalmazása nagy utat tett meg mostanáig, ugyanakkor az elmúlt években, valójában az elmúlt száz év eredményeire alapozva szintén nagy előrelépést tapasztalhattunk meg, immár a pontos és gyors azonosítást igénylő érintés nélküli biometrikus adatgyűjtés terén. A COVID-19 világjárvány következtében az érintés nélküli technológiát, a biometrikus adatgyűjtést alkalmazó rendszerek használata iránt megnőtt a kereslet. Az egyik legújabb és legszembetűnőbb érintés nélküli azonosításra szolgáló rendszer a norvég reptereken alkalmazott biztonságos áthaladást segítő technológia, amely biztosítja a poggyászfeladástól kezdve a beszállásig elkerülhető a fizikai kontaktus a személyzettel vagy a beléptető berendezésekkel. A norvég Avinor vállalat ezzel az intézkedéssel is szeretné növelni az utasok bizalmát, akik az online regisztrálás során megkapják a beszállókártyát.[339] Az intelligens poggyászfeladó automata segítségével elkerülhető a kontaktus. Budapesten, a Budapest Airport is alkalmaz hasonló technológiát. Egyes repterek robotok használatával is kísérleteznek, mint például a dél-Koreai Incheon nemzetközi repülőtér egy, utasokat arcmaszk viselésére emlékeztető robot tesztelését végzi. A robot rögzíti és továbbítja azon személyek arcáról készített felvételt, akik nem teljesítik a hatóság által előírt feltételeket. (Simple flying touchless airport technology COVID) A biometrikus adatgyűjtés alapú IT rendszerek tesztelésben például Németország, Kanada, Kína, Japán, Izland, Olaszország, Spanyolország is részt vesz, ezáltal jelentősen felgyorsítják az ellenőrzési folyamatot. További kezdeményezés, hogy az utasok egy speciális rendszerbe feltöltik a *szelfiket*, a hitelesített útlevéllel ezt ellenőrzik, majd a beszállókapunál egy képernyő segítségével megtörténik az azonosítás és beszállhatnak. Az automatizált határellenőrzési rendszer valószínű a COVID-19 után is velünk marad. További érintés nélküli megoldások születnek abból a célból, hogy biztosítsák a személy és

[338] Czuni László, Biometria a számítógépes személyazonosításban - vizuális módszerek, egyetemi jegyzet, Pannon Egyetem, Műszaki Informatikai Kar, Képfeldolgozás Kutatólaboratórium, 2015.
[339] Avinor Oslo Airport: A new border control solution by IDEMIA, International Airtorp review, 2019., Avinor rolls out end-to-end touchless travel programme, International Airtorp review, 2020.

vagyonvédelmet, ezáltal társadalmi távolságtartás mérése a reptereken és egyéb forgalmas helyeken, arcmaszkok viselésének detektálása, testhőmérséklet mérés, légszűrő rendszerek alkalmazása és fertőtlenítés, utasérkeztetés, vagy szigorúbb takarítási eljárások alkalmazása. Mindezen módszerek és eljárások használata drasztikusan csökkenthetik a személyes kapcsolattartások számát. Továbbá a mobilalkalmazások úgyszintén jelentősen csökkenthetik a kapcsolattartás szükségességét, de az applikációk használatával az ügyintézési és a személyes érintkezési kötelezettségek a minimálisra csökkenthetők. A mesterséges intelligencia technológiáját alkalmazó rendszerek esetében bármely érintés nélküli vezérlés hozzáadható minden egyes kiszolgáló eszközhöz, amely tovább fejlesztési lehetőséget biztosít. Ilyen például az emberi reakció érzékelése, feldolgozása és értelemzése, mint például a mozgáskorlátozott személyek esetében a fej mozgásával irányítható az adott önkiszolgáló eszköz. A hangfelismerő eszközök fejlesztésével, egyedi hangok, hangminták gyűjtésével, alkalmazásával és az egyének felismerésével betegellátó intézmények munkája is támogatható, vagy forgalmas helyeken az adott egyén hangja felismerhető. A gyors azonosítási technológia segíthet megakadályozni a kórokozók terjedését a repülőtereken, ezáltal a közlekedés is biztonságosabbá válik. A biometrikus adatok tárolása, feldolgozása és felhasználása különböző célokat szolgálhat. Az adatok használhatók kereskedelmi szolgáltatások (pénzfelvétel, hozzáférés ellenőrzés, számlázás, vásárlás, beléptetés) nyújtására, hatósági (személyazonosság igazolása, határátlépés, katonai programok, adathozzáférés) alkalmazások használatára, bűnügyi és bírósági ügyek intézésére és eljárások lefolytatására (halottazonosítás, bűnözők felderítése és azonosítása, emberi és vérszerinti kapcsolatok meghatározására, elveszett személyek felderítésére, bűntetővégrehajtásra és nyomkövetésre: börtön, javítóintézet, házi őrizet). Az előbb felsoroltakon kívül számos helyen magáncélból és közérdekből egyaránt alkalmaznak különböző biometrikus adatok detektálására információs eszközöket, így videó- és hangrögzítő, arcfelismerő, érintés nélküli újlenyomatolvasó, retinabeolvasó és felismerő rendszereket, amelyek alkalmasak a személyes adatok (arcpontok, kézlenyomat, hang, mozgás) rögzítésére és továbbítására, feldolgozás és további felhasználás céljából. Az alkalmazási területeket többféle képpen csoportosíthatjuk, mint például videófelügyelet (személy és vagyonvédelem céljából), egészségügy, illetve gyógyítás (orvosi kezelések, kórtörténet meghatározása, személyazonosítás, egészségügyi rendszerhasználat során azonosítás), munkáltatói ellenőrzés (munkaidőnyilvántartás: be- és kilépés ellenőrzése, azonosítás, rendszerhozzáférés ellenőrzés) céljából alkalmazott információs eszközök. A biometrikus adatok rögzítésének és tárolásának korlátaival és kihívásaival a vállalatok és az intézmények napi szinten szembesülnek. A

reptereken használt biometrikus rendszerek magukban foglalják a személyhez kapcsolódó regisztrációt, azonosítást és a tanúsítást, amellyel egy bizonyos személy azonossága igazolható. Az azonosítási folyamat alkalmával különböző információs rendszerek együttműködését, interoperabilitását biztostani kell, így a hatósági és a reptéri adatbáziskezelő, valamint alkalmazásrendszerek közti folyamatok biztosítását, a feladatainak biztonságos elvégzését és a kommunikáció biztonságát. A tudomány jelenlegi állása alapján az ujjlenyomat, az írisz, az arcvonalak vagy az emberi hang tulajdonsága ugyan megváltoztatható, de nagyon költséges és bonyolult orvosi módszer segítségével, ezért a biometrikus adatok kicserélése tömeges formában, a napjaink orvosi gyakorlata szerint nem megoldható. Tehát a biometrikus adatok tárolása, kezelése és továbbítása különleges biztonsági védelmet kíván, mivel azok egyediek, nem lecserélhetők és nem pótolhatók. Ugyanakkor egy személyi igazolványszám vagy egy információs rendszer felhasználói adatai bármikor megváltoztathatók. A biometrikus rendszerek iparági szakértői az érintés nélküli biometrikus adatokat kezelő rendszerek három formáját látják reálisnak: az arc-, írisz-felismerést vagy ujjlenyomat azonosítást. Az arcfelismerő rendszerek jellemzően négy komponensből állnak: képi rögzítésre alkalmas fényképezőgép, algoritmus az arc template létrehozására, adatbázis a képek tárolására, valamint algoritmus a képek összehasonlítására (a készített képre és a tárolt képekre vonatkozóan). Az arcfelismerő rendszerek működését az úgynevezett gépi tanulás (MI), a mélytanulás (deep learning) és a neutrális hálózatok technikái is támogatják.[340] A Google Picasa képszerkesztő szoftvere például arcfelismeréssel nevekkel címkézi a szoftver segítségével az adatbázisba betöltött fotókat. A Facebook szintén arcfelismerési funkciókat használ a kapcsolatok azonosításához és képes 98%-os pontossággal azonosítani a fényképeken szereplő személyeket az adatbázisuk segítségével. Az Amazon Prime Photos szoftvere nemcsak az arcokat vagy a tárgyakat ismeri fel, hanem az arcanalízis technológiával az egyének érzelmi állapotát tudja elemezni, úgymint a száj, szemöldök állása, tehát az egyén mosolyog vagy sem. Az Apple 3D arcszkennelő funkciója újlenyomat beolvasó helyett az arcfelismerő technológiát használja a bejelentkezéshez. Bár az emberi arc alakja, vonalai változnak, az arcfelismerő rendszereket ki kell egészíteni az öregedési folyamat által létrehozott változásokkal, illetve annak valószínűségével. További hibatényező lehet az arc megvilágítása, az éppen aktuális arckifejezés, vagyis mimika, a szemüvegviselés és az elmosódás. Az érintés nélküli ujjlenyomat technológiák (CFT - Contactless Fingerprint Technologies) használata potenciális előnyökkel

[340] Lawrence, Steve, et al. "Face recognition: A convolutional neural-network approach."IEEE transactions on neural networks8.1 (1997): 98-113.

jár az állami és a magánfelhasználók számára. A CFT technológiák nagymértékben javíthatják a felület által eddig begyűjtött adattartalom minőségét és drasztikusan növelhetik a gyűjtemény méretét is. Előnye az előző technológiához képest a gyorsabb és higiénikus adatrögzítés, mivel nincs szükség a fizikai érintésre. A CFT alkalmazása során 3D ujjlenyomat kép készül, ami a korábbi tinta, papír, lemez, optika vagy érzékelő felület alapú technológiával szemben hatékonyabbnak tűnik. A 3D technológia kiküszöbölheti a 2D technológiák által okozott eredmények torzulását, a szennyeződések (úgymint tinta elmosódás, papíron vagy érintőképernyőn szennyeződés) által okozott hiányosságokat, ezáltal gyorsabb a feldolgozás és hatékonyabb az azonosítás is. Az FBI által használt adatbázisából az ujjlenyomat-egyeztetés algoritmusát alkalmazó NGI[341] rendszere által a kezdetekben 92%-ban, ma már viszont 99,6%-os arányban azonosíthatók az egyének.[342] [343] Hasonló arányban változott az arcillesztési és –felismerési technológia eredményessége is, amely 92%-ról 97,5%-ra nőtt. A CJIS adattár központi rendszeréhez online kapcsolódó mobil azonosító eszköz gyors ujjlenyomat keresésre szolgál, amivel a tisztviselők másodpercek alatt megkaphatják az egyén összes elérhető adatát. Ez a RISC gyorskereső szolgáltatás hatékonysága többek között abban rejlik, hogy képes kevesebb, mint 10 mp alatt adatot szolgáltatni. Az adattár hozzáfér a Nemzeti Bűnügyi Információs Központ adattartalmához is, beleértve az elítéltek, jogsértők, terroristák, vagy gyanúsítottak, illetve eltűnt személyek adatbázisát. A biometrikus adatokat, úgymint újlenyomat, arcvonal felismerő technikákat felhasználják a laptop, telefon bejelentkezéséhez, majd további applikációhoz, úgymint banki tranzakciókhoz, szavazásokhoz, és egyéb ügyviteli rendszerekhez.[344] Az elmúlt tíz évben számos olyan biometrikus azonosításon alapuló információs rendszert vezettek be, amelyek esetlegesen nem a kellő módon teljesítik a magas információbiztonsági és adatvédelmi követelményeket. (facebook adatszivárgás) Sok esetben az állami felügyeleti szerveknek nincs rálátásunk a vállalatok által alkalmazott rendszertechnológiára, hiszen az egyedi technológia jogvédelem alá esik. Az állampolgárok kevésbé tájékozottak a technológiák megbízhatóságában, megfelelő működésében és a biometrikus adattárolásra és kezelésre vonatkozó információbiztonsági tanúsítvánnyal is rendkívül kevesen rendelkeznek. Mivel a kormányzati szervek és a kereskedelmi szervezetek egyre inkább arra törekszenek, hogy rögzítsék és adatbázisokban tárolják a biometrikus

[341] Next Generation Identification (NGI)
[342] FBI, Advanced Fingerprint Identification Technology (AFIT), https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi, letöltés: 2021. május 5.
[343] FBI, NGI, https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view, letöltés: 2021. május 5.
[344] Győrffyné Holló Krisztina, Az érintés nélküli adatgyűjtés kockázatai és a kockázatszámítás módszerei, DUNAKAVICS 9 : 8 pp. 77-97. , 21 p., 2021

adatokat, amelyek természetükből adódóan nem változhatnak így aggodalomra ad okot, hogy a felhasználásra vonatkozó előírások megfelelő szigorral rendelkeznek vagy sem. Mivel a biometrikus információinak tárolására adatbázisokat hoztak létre, és a kormányzati szervek ezt egyre jobban használják, ezek az adatbázisok immár célponttá váltak, és növekszik az adatvédelmi jogsértés kockázata. Az adatvédelmi jogokkal foglalkozó szervezet, az Elektronikus Adatvédelmi Információs Központ (EPIC)[345] felszólította a TSA-t, hogy vizsgálja meg a TSA Pre-Check alkalmazás biometrikus adatainak gyűjtési lehetőségeit.[346] Az EPIC aggodalmát a különleges adatnak minősülő biometrikus adatokhoz kapcsolódó azonosítók fokozottabb fenyegetettsége miatt fejtette ki, amelyeket az előzetes ellenőrzésre való jogosultság meghatározásán kívül más célokra is használnak. Jelenleg a TSA és a kormányzat számára is rendelkezésre áll a technológia, de figyelembe kell venni a magánélet befolyásolására vonatkozó tényezőket és az adatvédelmi előírásokat, mint például az adatok tárolásának minimalizálására vonatkozó adattakarékosság elvét (data minimisation principle), valamint a kormányzati adatbázisok biztonsági kockázatait is. Mivel a biometrikus adatok elérése vonzó a hackerek számára, ezért növeli a jogsértések számát, és az okozott kár mértékét. Számos napi használatban lévő informatikai eszköz, tehát telefon vagy laptop használ biometrikus azonosítást, aminek védelmi technológiája rejtett a nagyközönség, illetve esetlegesen a hatóságok számára is. A hitelesítési forgatókönyv szerint a hozzáférés biztonságos, mivel a biometrikus adat a felhasználó saját mobiltelefonján tárolható, és a használata önkéntes és korlátozható, ugyanakkor a biztonság érdekében a hozzáférés és az üzemeltetés szabályain is szigorítani kell. Kormányzati szintű alkalmazások terén több millió személy biometrikus információja kerülhet veszélybe, tehát a kockázat jelentős. A biometrikus adatok minden egyes ember számára egyediek, ha ezek veszélybe kerülnek az egyének magánéletét és biztonságát örökre befolyásolja. A biometrikus adatok gyűjtését, tárolását, felhasználását és továbbítását hazai és nemzetközi rendelkezések szabályozzák. Tekintettel arra, hogy a biometrikus adat, olyan különleges adat,[347] amely egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ezért az adatvédelmi szabályokon túl célszerű elvégezni az adott információs rendszerre a kockázatkezelést. A kockázatkezelés a kockázatmenedzsment[348] részét képezi. A

[345] Electronic Privacy Information Center, https://epic.org/
[346] Transportation Security Administration (TSA, USA), https://www.epic.org/apa/comments/EPIC-TSA-Pre-Check-Expansion-Comments.pdf, letöltés: 2021. május 5.
[347] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
[348] Som Zoltán, Kockázatmenedzsment gyakorlat, Nemzeti Közszolgálati Egyetem, 2014.

kockázatmenedzsment egy proaktív módszer a biztonsági kockázatok csökkentésére és a biztonsági teljesítmény javítására. A hatékonyan végrehajtott kockázatmenedzsment dokumentált, folyamatalapú és elősegíti a biztonságos működést. A legtöbb ágazat törekedett arra, hogy a saját területén a kockázatmenedzsment folyamatát alkalmazzák. A kockázatmenedzsment fázisai a következők: bevezetés, előzetes felmérés és elemzés, kockázatelemzés (kockázatazonosítás, kockázatbecslés és kockázatértékelés), kockázatkezelés és -javítás, valamint beavatkozás, hatásellenőrzés és mérés, továbbá kockázatelfogadás, és eredmények közzététele (kommunikáció). A kockázatmenedzsment célja, hogy a kockázatértékelés következtében megállapított kockázat, valamint a maradványkockázat a lehető legkisebb mértékű legyen. A kockázatkezelést folyamata mindaddig tart, amíg a kockázatot a lehető legkisebb mértékűre sikerül csökkenteni. Kockázatelemzés során figyelembe kell venni a szükséges intézkedések típusát, ami lehet megelőző (preventív), észlelő (detektív) és javító (korrektív). Az intézkedések típusának megválasztása esetfüggő, ezért az alkalmazható általános érvényű elveket, módszereket érdemes figyelembe venni. A kockázatkezelés során az incidenst kiváltó okokat, az incidens folyamatát és lehetséges kimenetét többféle módszerrel lehet vizsgálni. Mivel a legtöbb incidens összetett, ezért elemzésükhöz is többféle módszer szükséges. Minden egyes elemzés során számba kell venni az elemzéshez alkalmazott eszközöket, módszereket és egy-egy új modell bevezetése nem azt jelenti, hogy a régiek elavultak, inkább csak azok továbbfejlesztett változata alkalmasabb a feladat elvégzéséhez. Az alkalmazott módszerek és az általuk megfogalmazott elvek kiegészítik egymást. Minden kockázatkezelés egyedi, amely egyedi vagyonleltárral, sebezhetőségekkel, esetleges incidensekkel és intézkedésekkel rendelkezik, ezért a kockázatkezelés során a meglévő kockázatkezelési módszerek megfelelő kiválasztásával tökéletesíthető a kockázatkezelési intézkedési terv, és csökkenthető az esetlegesen bekövetkező incidensek száma és hatása, valamint a kockázat, hiszen az esemény bekövetkezésének valószínűsége is csökken, így növelhető a kockázatkezelés hatékonysága. Az alábbiakban felsorakoztatott módszerek segítenek abban, hogy a kockázatot a lehető legpontosabban határozhassuk meg. Kockázatkezelésnél az alábbi módszereket lehet figyelembe venni. Modellcsoportok lehetnek például biztonsági modellek és baleseti modellek. Biztonsági modellek, tekintetében a biztonságra (elsősorban ipari, informatikai, nemzet) vonatkozó tulajdonságokkal és feltételezésekkel kapcsolatos hipotéziseket rögzítik, amelyek igazolásával hozzájárulnak a rendszer biztonságának növeléséhez. Baleseti modellek, a baleseti hipotézisek összessége,

amely az előfordulásának módját és az elveket rögzítik, ilyen például a Seveso-irányelv[349] vagy az irányelv alapjául szolgáló modellek. A baleseti modellek egyik alapja az egyszerű, véletlenszerű, szekvenciális modell, a H. W. Heinrich dominómodellje (22. ábra), amelynek lényege, hogy a balesetek egy meghatározott sorrendben előforduló, mechanikus események sorozatából származnak és a baleset megakadályozható azzal, ha eltávolítjuk a dominósorozat egyik meghatározó tényezőjét.[350] A dominóelv a kockázatkezelés során jól alkalmazható, hiszen a megfelelően kiválasztott gyenge pont kezelése és a biztonsági rés befoltozása, ezért kutatásom információbiztonsági kockázatkezelésénél is alkalmaztam. Az adott sebezhetőség kijavítása a sebezhetőséget kihasználó incidensek számát csökkenti, mivel a támadás során ezen a helyen rést nem, csak bezárt ajtót találnak. A modell előnye, hogy egyszerű és könnyen átlátható, megérthető és lehetőséget nyújt a lényeges ok-okozati tényezők azonosítására, amelyek hozzájárulnak a baleset vagy incidens bekövetkezéséhez. A dominóelv a viselkedésalapú biztonsági programok együttes alkalmazásával lehetőséget nyújt a gyenge pont előtérbe helyezéséhez, az esetleges emberi hibák, hibás emberi teljesítmény észleléséhez. A dominóelv alapján a következő kockázati faktorok állapíthatók meg: a kiváltó ok (eredő tulajdonság) és társadalmi környezet (hanyagság, makacsság, kapzsiság; nem kívánatos vagy zavaró tényező), a személy hibája (veszély okozása, bármely emberi tulajdonságból vagy viselkedésből eredően), a nem biztonságos cselekmény és / vagy mechanikai vagy fizikai veszély, a baleset (főként emberi hibából eredő esemény, ami sérülést okoz), valamint a sérülés (sértés vagy sérülés, ami a baleset következménye). A H. W. Heinrich másik baleseti modellje a „biztonsági piramis" vagy „baleseti háromszög", amelynek teóriáját tovább gondolva megállapítható, hogy a kisebb események bekövetkezési gyakoriságának csökkentése, csökkenti a súlyos balesetek bekövetkezésének valószínűségét. A következő modell, amelyet kutatásom során szintén alkalmaztam, James Reason svájci sajtmodellje, amely szerint [351], ha feltételezzük, hogy az incidenst az aktív hibák (hibás biztonsági magatartás) és látens, környezeti tényezők kombinációja okozza, a korlátok megerősítésével megelőzhető a baleset. A biztonság menedzselése ebben az eseteben is megköveteli a teljesítmény-mutatókat. A módszer lényege, hogy az incidens csak akkor következhet be, ha minden „sajt" rétegen, azaz minden védelmi rendszeren átcsúszik a nemkívánt támadási kísérlet. Számos iparág, mint

[349] Seveso-irányelv, Veszélyes anyagokkal kapcsolatos súlyos balesetek, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l21215&from=HU, 1976-ban történt seveso-i katasztrófa következtében a balesetek megelőzésére és kezelésére vonatkozó jogszabály

[350] H.W. Heinrich, Industrial Accident Prevention, A Scientific Approach, Second edition, McGraw-Hill Book Company, New York and London, 1941.

[351] James Reason, Managing the Risk of Organizational Accident, Routledge, 1997.

például a közlekedés (légitársaságok) vagy az egészségügy használja ezt a modellt. A védekezési lehetőségeket a különböző méretű és elhelyezkedésű lyukakkal ellátott „sajtszeletek" jelentik. Lehetőleg azonos méretű és elhelyezkedésű lyukakkal ellátott „sajtszeletek" ne kövessék egymást. Amennyiben ez mégis előfordul, az adott védelmi réteg nem éri el a szükséges hatást és a támadás átjut rajta. Szükséges a gyenge pontok minimalizálása és a biztonsági rések befoltozása. A következő modell, amelyet szintén alkalmaztam kutatásom során, a Bow-tie, ami egy vizuális csokornyakkendő módszer a veszély hatásainak, a kockázatok, a következményeknek megértésére. A módszer lényege, hogy a bal oldalon fel kell sorolni az összes olyan lehetséges okot vagy fenyegetést, amely az esemény bekövetkezéséhez vezethet. A jobb oldalon pedig az összes olyan következményt fel kell tüntetni, amely az esetlegesen bekövetkezendő eseményhez kapcsolható. A kiváltó okok és a lehetséges következmények egymással összekapcsolhatók és az ok-okozat között felállítható a logikai folyamatábra. A Bow-tie modell továbbfejlesztett változata a HSE módszer, ami egy strukturált ellenőrzési modell a kockázatok kezelésére. A HSE módszert nem alkalmaztam kockázatkezelés során, ugyanakkor mint újabb verzió tekintetében említésre méltó. A Loss of control accident model, az irányítás elvesztése – a nem lineáris baleseti modell (French BEA – Bureau of Enquiry and Analysis for Civil Aviation Safety) feltételezése szerint, az incidens egy nem várt esemény és a normál teljesítményváltozás kombinációjából adódik. Az incidens megelőzése a folyamatok megértésében és a montírozásában rejlik. Az elvárt védelmi szint megköveteli a bekövetkezhető események detektálhatóságát és a megfelelő reagálás képességét. A modellt repülőgép balesetek analizálásához és megelőzéséhez használják.[352] A mentális típusú modellek alkalmazása befolyásolhatja az adott rendszer tervezését és működését, az operatív döntéseket és a munkavállalók viselkedését. A humán modell szerint a biztonság jelentősen javul, ha eltávolítjuk a „megromlott almát", tehát az olyan alkalmazottakat, akik emberi hibákat, úgynevezett „*human-error*"-t generálnak, mivel sorozatos gondatlan magatartásuk átterjed a többi munkavállalóra is. Bármely rendszerben az emberi viselkedést a környezeti tényezők, korlátok befolyásolják, mint például a nyereséges és veszteséges típusú folyamatok, biztonsági műveletek, munkaterhelés. A „*human-error*" menedzsment rendszerszemlélet híveinek egyik jelentős álláspontja, hogy egy átfogó irányítási programra törekszenek, amely több különböző célra irányul: a személyre, a csapatra, a feladatra, a munkahelyre és az intézményre.[353] (Humán faktor vizsgálata, az 5. fejezetben közölt

[352] Győrffyné Holló Krisztina, Az érintés nélküli adatgyűjtés kockázatai és a kockázatszámítás módszerei, DUNAKAVICS 9 : 8 pp. 77-97. , 21 p., 2021

[353] James Reason, Human error: models and management, 2000.

kutatási eredmények.) Kockázatkezelést segítő módszer az ALARP (As Low As Reasonably Practicable)[354] kockázatkezelési keretrendszer, amely a kockázatcsökkentés meghatározására szolgáló alapelveket rögzíti. Az Európai Unió számos döntési mechanizmusához,[355] vagy repülésbiztonság rendszereihez használják az ALARP keretrendszert, amelynek ismérvei az elfogadhatatlan tartomány, amely a tevékenységekhez kapcsolódó előnyöktől független, az elfogadható ALARP tartomány, ahol a kockázat vállalható, de van következménye. A javasolt kockázatkezelést akkor kell végrehajtani, ha a veszteség nincs aránytalanul nagyobb mértékben a végrehajtás által elért előnnyel szemben. A kockázati szintet a lehető legnagyobb mértékben csökkenteni kell, figyelembe véve annak költségének mértékét. Az általánosságban elfogadható tartomány esetében nincs szükség további kockázatcsökkentési módszer alkalmazására. Példaként megemlítendő továbbá a COSO-keretrendszer, amelyet az információbiztonsági kockázatkezelésnél nem használtam fel, viszont jelentős rendszernek tekinthető. A COSO-keretrendszert 1992-ben vezettek be az Amerikai Egyesült Államokban, és legfőképp vállalkozások használták. Azóta széles körben elterjedt és számos közszolgálati intézmény is alkalmazza az egységes belső ellenőrzési keretrendszert. A COSO ERM kockázatviselési szintje azt mutatja meg, hogy a vezetőség mekkora kockázatot tart elfogadhatónak, milyen mértékű lehet a kockázati tolerancia elsődlegesen a gazdasági tevékenységek figyelembe vételével. Az eseményeknek lehetnek negatív hatásúak, amelyek kockázatot jelentenek és megakadályozhatják az értékteremtést, illetve ronthatják a meglévő értéket, valamint lehetnek pozitív hatásúak, amelyek ellensúlyozhatják a negatív hatásokat vagy lehetőségeket jelenthetnek a szervezet számára. Pozitív és negatív hatású események kombinációja is előfordulhat. A keretrendszer pozitívan befolyásolja a célok elérését, támogatja az értékteremtést és az értékmegőrzést.[356] Rávilágít arra, hogy a lehetséges események milyen mértékben befolyásolhatják a vállalkozások és intézmények célkitűzéseit. Két szempont alapján értékeli a kockázatokat: valószínűség és hatás. A keretrendszer kvalitatív és kvantitatív kockázatértékelési módszerek kombinációját alkalmazza. [357] Kockázatértékelés matematikai számítási módszerei is jelentősek. A kockázatelemzés a rendelkezésre álló információk szisztematikus felhasználása a veszélyek azonosítására és az egyénekre, a tulajdonságokra, és

[354] Reece A. Clothier, Brendan P. Williams, Neale L. Fulton, XunGuo Lin, ALARP and the Risk Management of Civil Unmanned Aircraft Systems, 2013.
[355] Health and Safety Executive, https://www.hse.gov.uk/managing/theory/index.htm, letöltés: 2021. május 9.
[356] COSO Enterprise Risk Management – Integrated Framework, https://www.coso.org/pages/erm-integratedframework.aspx, letöltés: 2021. május 9.
[357] Az Európai Bizottság szervezetirányítási rendszere: helyes gyakorlatok?, www.eca.europa.eu/lists/ecadocuments/sr16_27/sr_governance_hu.pdf, 2016. Luxembourg, letöltés: 2021. május 9.

a környezetre gyakorolt kockázat becsléséhez. (IEC 60300-3-9, 1995) A kockázatértékelés a kockázatelemzés és a kockázatszámítás vagy becslés átfogó folyamata. A kockázatértékelés alapelvei szerint a kockázatszámítás leegyszerűsített számítási módja:

$$R = C \times F$$

ahol az R (Risk) kockázat egy adott incidens vagy esemény bekövetkezésének gyakorisága vagy valószínűsége (F), valamint a következmény súlyosságának (C) [358] a szorzata.

Komplex rendszerek esetén alkalmazandó az alábbi számítási módszer

$$r = \sum_{t \in T} (p_t \times d_t)$$

ahol r – a rendszer biztonsági kockázata, T – a releváns fenyegetések halmaza, p_t – egy adott fenyegetés bekövetkezésének valószínűsége (gyakorisága) és d_t – egy adott fenyegetés bekövetkezéséből származó kár.[359]

A kockázatszámítási módszerek lehetőséget biztosítanak a kockázat gyors értékelésére, ezáltal lehetőség van egy adott rendszer információbiztonsági kockázatainak felmérésére és meghatározására, valamint szükséges intézkedések megvalósításával az elvárható és elfogadható kockázati szint beállítására. A kockázati mátrix szintén felhasználható a kockázatkezelés során, amely olyan kétdimenziós diagramm, melynek függőleges tengelyén a veszélyeztető hatás következménye, vízszintes tengelyén a veszélyeztető hatás bekövetkezési valószínűsége (gyakorisága) található, és amelynek eredményeként megállapítható, hogy egy adott veszélyeztető hatás mekkora kockázatot jelent az adott rendszerre, objektumra.[360] [361] Számos matematikai számítási módszer szolgál a kockázatelemzésre, a maradványkockázat, valamint a hiba számosságának, úgymint a hibás folyamatok számosságának megállapítására, amely a rendszer biztonsági szintjének kvantitatív értékelését eredményezi. Ezekhez a módszerekhez összetettebb matematikai számítási folyamatok szükségesek, amelyekhez felhasználható a HAZOP – Hazard Operability Analysis, a HACCP – Hazard Analysis and

[358] Marvin Rausand, Risk Assessment Theory, Methods, and Applications, New Jersey, 2011.,
„*Frequency analysis. This step will usually involve a deductive analysis to iden-tify the causes of each hazardous event and to estimate the frequency of the hazardous event based on experience data and/or expert judgments.*"
„*Consequence analysis. Here, an inductive analysis is carried out to identify all potential sequences of events that can emerge from the hazardous event. The objective of the inductive analysis is usually to identify all potential end consequences and also their probability of occurrence.*"
[359] Muha Lajos, Az informatikai biztonsági kockázatok elemzése, Robothadviselés, 2009.
[360] 234/2011. (XI. 10.) Korm. rendelet, a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról, 2021. május 9-i állapot
[361] NASA, Risk Management Reporting, 2009.

Critical Control Points, az FMEA – Failure Mode Effects Analysis, vagy az FMCEA – Failure Mode, Effects and Criticality Analysis. Általánosságban megállapítható, hogy a hibák száma fordítottan arányos a biztonsági szint értékével. Az előbb említett módszeret információbiztonsági kockázatkezelés során háttérkutatáshoz használtam, az értekezés szempontjából kevésbé jelentősek, tehát ezek bővebb kifejtése az értekezésnek nem témája. Szervezetre vonatkozó input erőforrások, amelyeket a rendszer a folyamatok és műveletek végrehajtása során felhasznál, valamint a környezeti hatásokat és kapcsolatokat, tehát a rendszeren kívülről érkező hatásokat, amelyek meghatározzák a szervezetek fenyegetéseit és a potenciális veszélyek jellegét és szintjét, a káros hatások bekövetkezésének valószínűségét, a megszakítások (rendellenes rendszerleállás, szolgáltatáskimaradás) szintjét és a helyreállítás költségét, valamint a kockázatok kezelését szolgáló ellenőrzések hatékonyságát. A személyes adatok adatkezelése során, tehát a legújabb, érintés nélküli biometrikus adatgyűjtésnél is ugyan úgy figyelembe kell venni az adatvédelmi és az információbiztonsági előírásokat. Tekintettel arra, hogy a biometrikus adatok az adatvédelemi szabályok és alapfogalmak szerint különleges adatnak minősülnek, fokozottabb védelmet kívánnak. A biometrikus adatokat gyűjtő vállalatok esetenként elhanyagolják az információbiztonsági kockázatok felmérését és kezelését, ezáltal az intézkedési tervekből és a fejlesztésekből kimaradhatnak azok a tényezők, legfőképp a jelentős biztonsági rések kezelésére irányuló intézkedések, amelyek az incidensek elkerüléséhez, megelőzéséhez vezethetnek. Információbiztonsági szempontból tehát elengedhetetlen azon információs rendszerek kockázatkezelése, amelyek személyes adatokat gyűjtenek, tárolnak és kezelnek. A kockázatok felmérésére, analizálására és kockázatértékelésre az elmúlt évtizedek során többféle, sokszor egymásra épülő, az információs technológiával szinte együtt fejlődő, számos modellt és módszert találhatunk, amely az adott információs rendszer esetében releváns lehet.[362] A megfelelő, de speciális módszer kiválasztása mindig rendszerfüggő vagy iparágfüggő, hiszen más módszereket alkalmaz a repülésbiztonság, az egészségügy vagy a közigazgatás. A tanulmányban azon módszereket emeltem ki, amelyek alapelveit tekintve számos területen lehet használni, ezáltal alkalmazásuk is népszerűbb. Azon alapelvek és módszerek, amelyek legjobban szolgálják az alkalmazásuk célját, elősegítik a hatékony információbiztonsági kockázatkezelést, költséget takarítanak meg az adott szervezet számára és az incidensek bekövetkezésének valószínűségét is csökkentik, közvetett módon pedig az információs rendszer biztonsági szintét növelik. Amennyiben a vállalatok és

[362] Krisztina Győrffyné Holló, Adam Karisztl, Domino effect and other models in the IT process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

intézmények támogatják az információbiztonsági kockázatkezelési intézkedések hatékony végrehajtását, az érintett a biometrikus adatát is nagyobb biztonságban tudhatja.

4.2.2.2. AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATKEZELÉST TÁMOGATÓ SZABÁLYOZÁSI TÖREKVÉSEK

„*Minél nagyobb méreteket ölt a digitalizáció és az összekapcsoltság, annál nagyobbak a kiberbiztonsági kockázatok is, melyek a társadalmat egészében véve sebezhetőbbé teszik a kiberfenyegetésekkel szemben, az egyes felhasználókra leselkedő veszélyeket pedig súlyosbítják, ideértve a sérülékeny felhasználókat, például a gyerekeket is. Az említett kockázatok csökkentése érdekében az uniós kiberbiztonság fokozására irányuló minden szükséges intézkedést meg kell hozni azért, hogy a hálózati és információs rendszerek, a távközlési hálózatok, valamint a polgárok, a szervezetek és a vállalkozások – a 2003/361/EK bizottsági ajánlásban (4) meghatározott kis- és középvállalkozásoktól (kkv) a kritikus infrastruktúrák üzemeltetőiig terjedően – jobban védve legyenek a kiberfenyegetésekkel szemben.*”[363] Az 5. fejezetben közölt kutatási vizsgálati eredményeim igazolják, hogy az internetes támadások egy része megelőzhető a felhasználói szféra információbiztonsági tudatosításával, nemzeti információvédelmi intézkedésekkel; hálózati, hardver és szoftver szabályozási rendszerének kialakításával és szigorításával, Európai Uniós irányelvek és hazai szabályozási rendszer kialakításával, működtetésével és betartásának ellenőrzésével. A hazai szabályozási rendszer kialakításában és támogatásában több hatóság és intézmény vesz részt.

4.2.2.3. A NEMZETBIZTONSÁGI SZAKSZOLGÁLAT NEMZETI KIBERVÉDELMI INTÉZET TÁJÉKOZTATÁSAI

A Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatásai a nemzeti információbiztonságot megerősítő jelentőségűek. Az esetek kiemelésével és figyelemfelkeltéssel az információbiztonsági megelőzés elősegíthető és csökkenthetők az incidensek száma. A kockázati tényezők és az intézkedési tervek feladatai beépíthetők az intézményi szabályozási és információs rendszerbe, tehát eljárás és gyakorlati jelentőséggel bír. Az NBSZ NKI figyelmeztetései az informatikai sérülékenységeket, kártékony kód leírásokat, riasztásokokat és egyéb tájékoztatásokat helyezi előtérbe. Honlapján és közösségi médiában rendszerüzemeltetők és egyszerű felhasználók számára elhelyezett hasznos és figyelemfelkeltő

[363] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:32019R0881, letöltés: 2022. február 20.

tanácsokkal és kiadványokkal, valamint tudástárral támogatja az információbiztonsági-tudatosság fejlesztését. A közösségi médiában megjelenő hirdetései nem reklám célzatúak, hanem incidensek statisztikai adatgyűjtése és incidensbejelentés alapján megállapított és közzétett információbiztonsági figyelmeztetések.

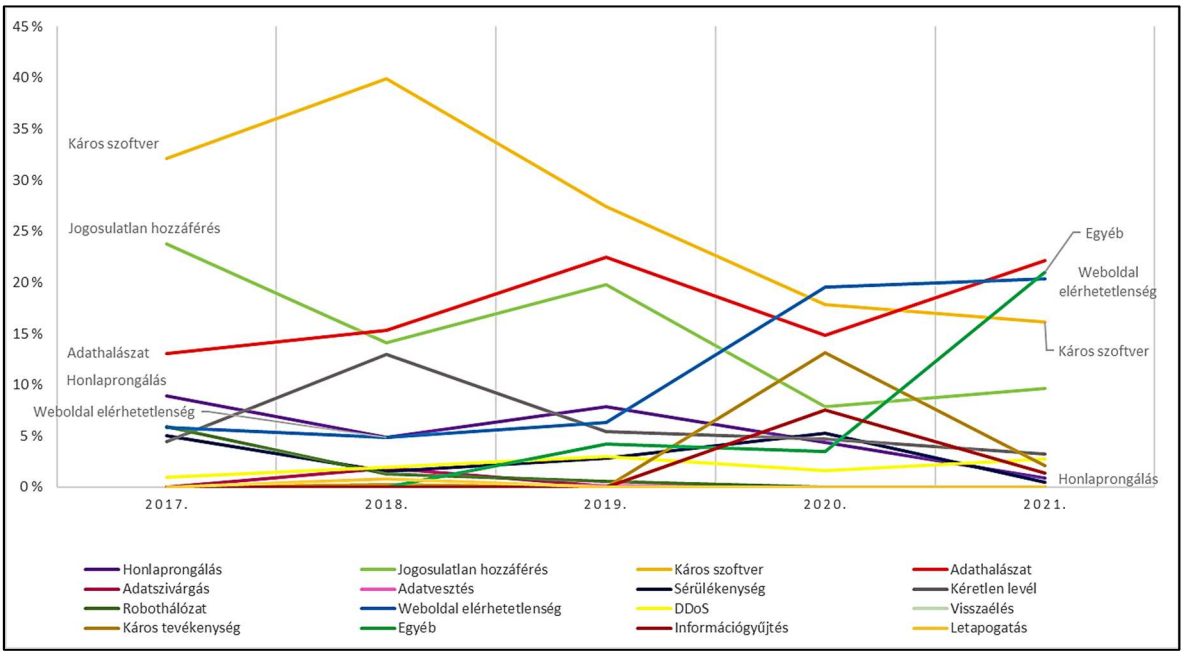
4.3. RÉSZÖSSZEFOGLALÁS

A biztonságtudatosság tanulmányozásához elengedhetetlen a kitekintés a kibertérre. A kibertér, amely a többféle megvilágítás szempontjából lehet egy virtuális világ, egy hálózati tartomány vagy egy kommunikációs csatorna, amelyben az internetet használók különböző személyes és vállalati, ipari vagy egyéb titkos adatokat tartalmazó adatbázisokkal teremtenek kapcsolatot, profilokkal alkotnak különböző virtuális közösségeket. Az internetes közösségek kialakulásával nemcsak a virtuális kapcsolatteremtést és más előnyöket szerezhetnek a felhasználók, de egy-egy lehetőség megjelenése után nem kell sokáig várni a bűnelkövetők megjelenésére se. Egyre tökéletesebb módszerekkel okoznak kárt online vagy internetes kapcsolattal rendelkező rendszereinkben és adatbázisainkban, adott esetben értékeket tulajdonítanak el vagy haszonszerzés célzattal felhasználják azt. A kiberbűnözők meglepő gyorsasággal adaptálódnak egy-egy új környezethez és az internetet használók körében egyre több az áldozatok száma, egyre nagyobb gazdasági kárt okoznak. Az internet, amely az online tér lehetőségeit nyújtja, a rendkívüli sok előny mellett rengeteg kockázati tényezőt jelent.

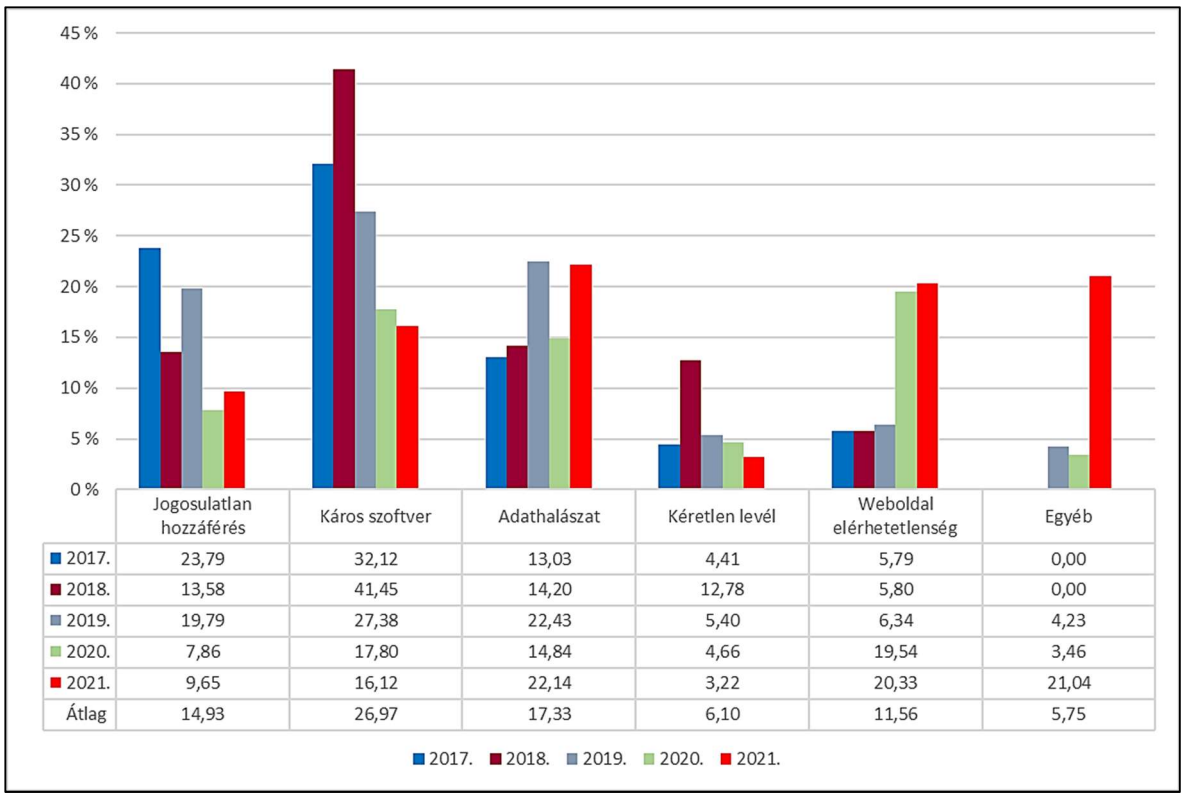
A kibertámadásokat és körülményeit nemcsak a nemzeti kibervédelemre szakosodott állami és civil szervezetek, az információbiztonságban vagy –védelemben tevékenykedő kutatók vizsgálják. Habár összességében elmondható, hogy humán eredetű kritikus tényezők tekintetében megfelelő teljesítési szinttel is rendelkezünk, a kibérvédelemre, kockázatmenedzsmentre fordított erőfeszítés nem állhat meg és a folyamatos tudatosítás is rendkívül fontos. A sérülékenységekből és a fenyegetésekből adódó kockázati tényezők felderítéséhez és kezeléséhez fegyelmezett biztonságtudatos felhasználói szférára és folyamatos továbbképzésre van szükség. A különböző szintű biztonságtudatos vagy a hiányos biztonságtudatos magatartás visszahat az adott intézmény informatikai rendszereire, annak biztonsági beállítására és az intézmény biztonságtechnikai intézkedéseire, valamint közvetett módon gazdasági fejlődésére. Így van ez a közigazgatás területén is. Bár az információbiztonságot vizsgálva a nemzetbiztonság vagy az ipar kerül elsődlegesen előtérbe, a közigazgatás területén is fontos az adatvédelem, a biztonságtudatosság és a kockázatkezelés. A közszolgálati információs rendszerek kommunikációjához elengedhetetlen az az

interoperabilitási stratégia, amely a rendszerek interoperabilitási képességének fejlesztésére irányul, és egyben figyelembe veszi az információbiztonsági alapelvek követelményeit is. A követelmények teljesítésével növelhető a rendszerek információbiztonsági szintje és a fenyegetések kivédésének aránya. Az Ibtv. értelmében fenyegetésnek kell tekinteni minden célzott támadást vagy támadási kísérletet vagy támadást, és biztonsági eseménynek vagy incidensnek, amennyiben a támadás a kívánt célt elérte. A törvény szerint fenyegetés minden, olyan lehetséges művelet vagy esemény, mulasztással járó cselekmény, amely sérti vagy sértheti az adott elektronikus információs rendszert vagy az elemeinek védettségét, biztonságát. A kiberteret ért fenyegetések analizálása és tudatosítása természetesen nem indok arra, hogy az ipari, informatikai technológiai fejlődést és növekedést meggátoljuk. Az egyre nagyobb és szélesebb körben terjedő e-közigazgatás, a szolgálatatás szempontjából keletkezett, valamint a felhasználói igény is arra mutat, hogy indokolt és elengedhetetlen a kibertér által nyújtott lehetőség optimális és tudatos kihasználása és használatának nagymértékű terjesztése. A jelen fejezetben megjelenített statisztikai adatok az elmúlt 8-10 év nemzetközi és hazai információbiztonsági incidensei összesített információiból származnak. A kutatásom során információbiztonsági szempontból külön vizsgáltam a GDPR és az Infotv. rendelkezéseinek életbe lépése előtti és utáni időszakot, és figyelembe vettem a COVID-19 világjárvány eseményeinek információbiztonságra gyakorolt hatását. A kutatásomhoz felhasználtam a nemzetközi és hazai tudományos, hatósági és információbiztonsággal foglalkozó nagyvállalatok által összeállított statisztikai adatokat. Kutatásom során megvizsgáltam a hazai NBSZ NKI által összegyűjtött incidensek és statisztikai adatait[364] és a jelen fejezetben külön összegeztem a két időszakra vonatkozókat. (13. ábra)

[364] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, IT-biztonsági sajtószemle, https://nki.gov.hu/it-biztonsag/kiadvanyok/sajtoszemle/, Időszak: 2017-2021., Hozzáférés ellenőrzése: 2022. augusztus 7.



13. ábra, Incidenstípusok eloszlása NBSZ NKI statisztikai adatai alapján - 2017-2021. saját adatgyűjtés, vizsgálat alapján saját szerkesztés



	Jogosulatlan hozzáférés	Káros szoftver	Adathalászat	Kéretlen levél	Weboldal elérhetetlenség	Egyéb
2017.	23,79	32,12	13,03	4,41	5,79	0,00
2018.	13,58	41,45	14,20	12,78	5,80	0,00
2019.	19,79	27,38	22,43	5,40	6,34	4,23
2020.	7,86	17,80	14,84	4,66	19,54	3,46
2021.	9,65	16,12	22,14	3,22	20,33	21,04
Átlag	14,93	26,97	17,33	6,10	11,56	5,75

14. ábra, Leggyakoribb incidenstípusok statisztikai adatai NKI adatai alapján - 2017-2021. saját adatgyűjtés, vizsgálat alapján saját szerkesztés

A kapott eredmények alapján megállapítottam, hogy a hazai viszonylatban, az elmúlt öt évben a káros szoftverek aránya csökkenő, a weboldal elérhetetlenség növekvő, a jogosulatlan hozzáférések csökkenő, valamint az adathalászat és az egyéb (nem nevesített) incidenstípusok növekvő tendenciát mutattak. Az időszakra vonatkozó incidenstípusok közül a káros szoftver átlaga: 26,97%, az adathalász tevékenység 17,33%, jogosulatlan hozzáférés 14,93%, míg a weboldal elérhetetlenség 11,56%, a kéretlen levelek 6,10% és az egyéb (nem nevesített) 5,75% volt. (14. ábra) A kapott incidenstípusok értékeit összevetettem az incidensek és az adatvédelmi jogsértések esetleírásával, az információbiztonsági irányítási rendszer szabványának, valamint az IBtv., GDPR és Infotv. rendelkezéseinek előírásaival és megállapítottam, hogy az incidensek bekövetkezésének egyik befolyásoló tényezője a „humán faktor", amely jelentős mértékben jelen van a káros szoftver elkészítésénél (támadói oldalon) és aktivitásának figyelmen kívül hagyásánál, valamint mulasztásnál (hiányos szakértelem, szabályok figyelmen kívül hagyása rendszerüzemeltetői oldalon), az adathalász üzenetek elkészítésénél (támadói oldalon) és üzenetek fogadásánál, valamint kért adatok továbbításánál (szabályok figyelmen kívül hagyása, hiányos információbiztonsági tudatossággal rendelkező felhasználó). A „humán faktor" és az az információbiztonsági tudatosság jelentőségével és az adott információs rendszerre gyakorolt hatásának vizsgálatával, valamint a kapott eredmények bemutatásával a következő fejezetben foglalkozom. A második hipotézisem (H2) szerint feltételeztem, hogy a felhasználói információbiztonsági tudatosság hiánya, amely az emberi tévedést és szándékos kárt eredményezhet, elősegíti az incidensek bekövetkezését, és támogatja a kiberbűnözést. Az ismertetett statisztikai adatok rámutatnak arra, hogy a kiberbűnözés legfőképp az adathalászat és a káros szoftverek tekintetében jelentős mértékű, és számottevő károkat okozott. A károk helyreállítása és a védelmi szint megerősítése jelentős anyagi ráfordítással járt, tehát gazdaságkárosító tényező. ENISA ETL jelentése szerint bár az elmúlt két évben tovább nőtt a információbiztonsági támadások száma, a hibrid irodai modell növelte a támadási felületet[365], valamint nehezítette a kibervédelmi szakemberek munkáját és az egyre növekvő felhőmegoldások alkalmazása a kiberbűnözőkre ösztönző hatással volt, ugyanakkor a szabály alapú (ISO 27001, GDPR, Infotv, IBtv. együttesen) informatikai és információbiztonsági fejlesztések, az interoperabilitási lehetőségek, a mesterséges intelligencia (MI) technológiáinak együttes alkalmazása nagyobb védelmet nyújt adatainknak, és rendszereinknek egyaránt, az egyre növekvő, kifinomult támadások kivédése ellen, továbbá az incidensek hatását (mentés és visszatöltés teszt, szimuláció, tudatosítás, router és szerver konfiguráció fejlesztése, kéretlen

[365] ENISA Threat Landscape 2021.

levelek jelölése MI módszerekkel stb.) is gyengíti. Ezen álláspont a H2 hipotézisem igazolásához is kapcsolódik, mivel igazolható, hogy az információbiztonsági rendelkezések alkalmazása hatékonyan befolyásolja az információs társadalom fejlődését.

A harmadik hipotézisem (H3), amely szerint feltételeztem, hogy a Magyarországon érvényes és intézményi adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését és a szervezet információbiztonsági tudatosság szintjét, az információbiztonsági kockázatkezelési módszerek alkalmazásával igazolható. A jelen fejezetben bemutattam az ISMS információbiztonsági kockázatkezelés elkészítésére vonatkozó szabályokat, eljárásokat és releváns módszereket, de a tényleges kockázatkezelési eljárást és vizsgálatot, valamint eredményeit a „humán faktor", mint befolyásoló tényező jellemzésével együtt ismertetem a következő fejezetben. Az ISMS kötelező eleme a kockázatkezelés lefolytatása és a munkavállalók rendszeres információbiztonsági tudatosítása (továbbképzések, tréningek, vezetői és csoportmegbeszélések). A jelen fejezetben hivatkozott incidensek leírásával és a vonatkozó statisztikai adatokkal is alátámasztható, hogy az incidenst szenvedett intézmények jelentősebb figyelmet szentelnek az adatvédelmi és információbiztonsági követelmények betartásának és finanszírozásának, az ISMS bevezetésének és működtetésének. Az elmúlt 8-10 évben, legfőképp a támadást szenvedett kormányzati szervek és nagyvállalatok, felsőoktatási intézmények nyilatkoztak úgy, hogy a bekövetkezett incidensek után nagyobb figyelmet fordítanak a kibervédelemre, és jobban figyelembe veszik, illetve finanszírozzák a szükséges információbiztonsági előírásokat. Tehát a vizsgálat során figyelembe vett intézményekre általában elmondható, hogy elkötelezettek az ISMS bevezetésére, az információbiztonsági szabályok szigorítására és a felhasználói biztonságtudatosság fejlesztésének támogatására. A következő fejezetben statisztikai adatokkal is igazolom, hogy a H4 hipotézis tekintetében a szervezetek által bevezetett ISMS, az információbiztonsági alapelvek és rendelkezések tudatosítása valóban hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését és a szervezet információbiztonsági tudatosság szintjét vagy sem.

5. AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG SZEREPE, HELYZETE, ÉS HATÁSA

5.1. AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG JELENTŐSÉGE

Az információbiztonsági tudatosság szintjének meghatározása hátterében rendkívül bonyolult, összetett folyamat áll, aminek kimenete általában egy adott pillanatban, adott környezeti tényezők által meghatározott helyzetben mért, sokszor az adott tudásszintre és szubjektív megítélésre épített eredmény. Ezen típusú tudatossági szint meghatározásának alapja lehet például kérdőív, tudásszint értékelés (vizsga, beszámoló) vagy csoportos trénig és interaktív, ötletelési módszerek alkalmazása. Az említett módszerek eredménye kiegészíti az adatvédelmi hatásvizsgálat és az információbiztonsági, különösen a hardver- és szoftverműködésből, sérülékenységvizsgálatból és incidensfelmérésből származó, statisztikai eredményeket. Az említett szubjektív és az objektív alapokra épített statisztikai adatokra egyaránt szükség van ahhoz, hogy reális jelen és jövőképet kapjunk az adott tudásszint és a fejlesztendő területek meghatározásához. A disszertáció negyedik és ötödik fejezetében bemutatott, valamint a kutatásom során, információbiztonsági felmérésből, kockázatelemzésből és –kezelésből származó objektív statisztikai adatokra összpontosítottam, és figyelembe vettem a nagyvállalatok által készített hiteles, de szubjektív felméréseket is. A felmérések alapján kiválasztottam néhány adatvédelmi jogsértést, amelyen keresztül szándékozom bemutatni a statisztikai eredmények igazolását, az információbiztonsági-tudatosság szintjének és a fejlesztendő területek meghatározását. Az adatvédelmi jogsértések elemzéséhez szükséges volt az úgynevezett „*humán faktor*”-ra vonatkozó empirikus módszer alapú kutatás lefolytatása, lényegi elemeinek bemutatása és elemzése. A „*humán faktor*” jelentőségének hangsúlyozásakor nem pszichológiai és szubjektív alapú, elemzéseket vettem figyelembe, hanem a bekövetkezett balesetek elemzéséhez kapcsolódó, hivatkozott szakirodalmat. A kockázatkezelésre vonatkozó kutatásom során az intézkedéseket kizárólag úgy tudtam meghatározni, ha feltérképeztem az incidensek lehetséges *humán* tényezőit. Egy-egy megelőző intézkedésnél, szabályok szigorításánál nemcsak a technikai megoldásokat és sérülékenységeket kellett figyelembe venni, hanem a támadók és a munkavállalók lehetséges reakcióit is. A megelőző intézkedéseket legtöbb esetben a lehetséges válaszlépések szimulációja és azok vizsgálata követte. A vizsgálatra azért volt szükség, hogy reálisan eldönthessem, melyik megelőző intézkedés lehet releváns és hatékony egyszerre. A vizsgálat során a vizsgálatban részt vevő szervezetnél a legtöbb intézkedéshez tudatosító módszereket

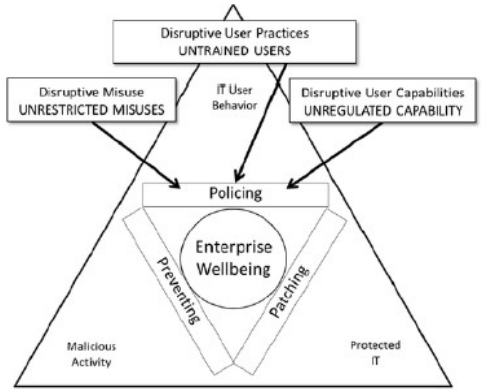
alkalmaztunk annak érdekében, hogy az intézkedések hatékonyságát növeljük. A hatékonyságot minden évben egy alkalommal megvizsgáltam és megállapítottam a tudatosítás által befolyásolt, az adott szervezetre vonatkozó információbiztonsági kockázatok javulásának tendenciáját, amit a jelen fejezetben részletesebben is ismertetek. A fejezet részei közé tartozik a nemzetközi viszonylatban meghatározott és a kutatásom során vizsgált hazai szervezet által, statisztikai adatokkal alátámasztott tudatosítás jelentőségének bemutatása és a digitális kompetencia fejlesztésének szükségességét alátámasztó, valamint az Európai Adatvédelmi Testület, a NAIH és saját kutatásból származó, publikált, a digitális kompetenciafejlesztést, az információbiztonsági-tudatosítást elősegítő útmutatók ismertetése. A „*humán faktor*", az információbiztonsági kockázatkezelés kutatási eredményeim, valamint az információbiztonsági-tudatosításra vonatkozó útmutatók ismertetése a harmadik és a negyedik hipotézis igazolásához szükségesek. A harmadik (H3), amely szerint feltételeztem, hogy a Magyarországon érvényes és intézményi adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését, valamint a negyedik (H4) hipotézisem, amely szerint feltételeztem, hogy az információbiztonsági tudatosítás rendszerét nemcsak az informatikai oktatásban, hanem minden korosztály számára elérhetővé kell tenni és minden szakterületen indokolt bevezetni és működtetni. A fejezetben található kutatási eredmények közléséhez és a háttérkutatáshoz dokumentum- és tartalomelemzési, információbiztonsági és kockázatkezelési módszereket, összehasonlító, statisztikai valamint egyéb adatelemzéseket, továbbá empirikus kutatást, a matematikai logika alkalmazását használtam.

5.2. A „*HUMÁN FAKTOR*" JELENTŐSÉGE

Napjaink technológiai forradalmát a gyors változás, a műszaki, illetve információs rendszerek dinamikus fejlődése jellemzi. Az ember kiszámíthatatlan aktivitása időnként komoly aggodalmat okoz az IT rendszerek biztonságának fenntartásában. A „*humán faktor*", és a „*human error*" azonosításához és elemzéséhez általában ipari balesetek, úgymint bányakatasztrófák, gyártás során bekövetkezett balesetek vagy közlekedési balesetek elemzését használják fel.[366] Az információbiztonsági incidensek és az ipari balesetek közti hasonlóság az események folyamatában keresendő. Az előbbiek tekintetében különösen személyes, ipari, kutatási vagy gazdasági adatok, míg az utóbbi esetekben főként ipari vagy személyt ért

[366] HSC (1993) Organising for Safety, 3rd Report of the Human Factors Study Group of the Advisory Committee on the Safety of Nuclear Installations, HSE Books

balesetek állnak az incidensek központjában. A katasztrófák elemzéséből származó általános alapelveket és következtetéseket az információbiztonsági kockázatkezelésnél is kiválóan lehet hasznosítani. Mivel a folyamatok, rendszerek tervezésében, kivitelezésében és működtetésében, valamint irányításában az emberi tényező elengedhetetlen, ezért az incidensek szempontjából a „*humán faktor*" vizsgálata nélkülözhetetlen. A rendszerszemléletű szervezetek rendszerint számolnak azon emberi aktivitásokkal, amelyek esetlegesen növelik a negatív események bekövetkezésének valószínűségét, lassabb termelékenységet és megnövekedett hibaarányt okoznak. A következő matematikai kutatási eredmény is azt bizonyítja, hogy az információbiztonság kockázatainak vizsgálatakor figyelembe kell venni a védeni kívánt információs rendszeren és a kártékony tevékenységen túl a felhasználói viselkedést.[367] (15. ábra)



15. ábra, IT infrastruktúrát befolyásoló tényezők

Az emberi tényező vizsgálatánál természetesen nem tudunk minden egyes tényezőt számba venni, de a releváns főcsoportok megállapíthatók. A releváns csoportok elemzéséből pedig algoritmus segítségével mérhető az emberi aktivitás – legyen az pozitív vagy negatív, tehát káros az adott információs rendszerre, ezáltal a szervezet működésére –, és a potenciális információbiztonsági képességek számszerűsíthetők.[368] A számítási módszer a kockázatok értékeléséhez és javításához nyújt segítséget. Az értékek meghatározásához elengedhetetlen az

[367] Hadarics, K., Gyorffy, K., Nagy, B., Bognar, L., Arrott, A., Leitold, F., Mathematical Model of Distributed Vulnerability Assessement, Security and Protection of Information 2017, University of Defence, IDET BRNO, Czech Republic, 2017

[368] Ferenc Leitold, Krisztina Győrffyné Holló, Zoltán Király, Quantitative metrics characterizing malicious samples, In: Cyril, Onwubiko; Pierangelo, Rosati; Aunshul, Rege; Arnau, Erola; Xavier, Bellekens; Hanan, Hindy; Martin Gilje, Jaatun (szerk.) Cyber Science, CyberSA for Trustworthy and Transparent Artificial Intelligence (AI), Dublin, Írország: Center for Multidisciplinary Research, Innovation and Collaboration 2021. pp. 82-83., 2 p.

emberi tényezők csoportjainak, és legfőképp az emberi hibák vizsgálata. Ugyanakkor az incidensek emberi hibáinak megítélése lehet téves alapú, ami az elemzés szempontjából hibás végkövetkeztetést eredményez. A téves megítélést már a vizsgálat elején ki kell zárni. Emberi mulasztás esetén téves döntés lehet, különösen ha elfogadjuk, hogy az emberi tévedés elkerülhetetlen volt, vállat vonunk, és az okozót csupán óvatosságra intjük, vagy ha nyilvánosan megnevezzük a felelőst, figyelmeztetjük, esetleg elmarasztaljuk, illetve végül felmerül a bizalomhiány, amely során egy átképzés, vagy akár sorozatos továbbképzés kiaknázása, majd egy esetleges eredménytelenség bekövetkezése sorszerű bukáshoz vezet. Az említett hibakezelés módszere önmagában haszontalan, mivel a hiba valós oka nem kerül előtérbe, és a megoldás sem megfelelő. Az adott eset teljes körű vizsgálata, csak a kiváltó tényezők és következmények feltárása adhat kielégítő eredményt. A HSC esetei és vizsgálatai az említett problémafelvetésen túl igazolták az Egyesült Királyságban bevezetett szabályozási rendszer jelentőségét és hatékonyságát, továbbá megerősítették, hogy a jó szándék önmagában kevés, azt szabályozott keretek között, gyakorlattá és ellenőrzött valósággá kell fejleszteni, annak érdekében, hogy a gyengeségek felszínre kerüljenek, és egyúttal a baleseteket megelőzhessék. A katasztrófákból levont általános következtetés lehet, ha a balesetek bekövetkezése előtt a biztonsági eljárásokkal, annak szervezésével vagy irányításával kapcsolatban kétely nem fogalmazódott meg, ezáltal az esetleges gyengeségek elrejtve maradtak. A baleset közvetlen okait tágabb összefüggésében, környezetben kell értelmezni, mint amelyben bekövetkezik. A rendszerek és berendezések tervezésére, és a biztonsági előírásokra nagyobb figyelmet kell fordítani, ezáltal minimalizálható az emberi tévedés lehetősége. Továbbá a tettek legyenek erőteljesebbek, mint a szavak. Az írásos biztonsági irányelvek, a részletesebb biztonsági szabályok és eljárások értelmetlenné válnak, ha nem rendelkeznek teljes, tehát anyagi, eszköz- és humánerőforrással, valamint szigorúan végrehajtási és rendszeres ellenőrzési stratégiával, megvalósítással. A vezetői irány- és példamutatás, úgymint például az elkötelezettség, a pozitív biztonsági attitűd és a motiváció, az egész szervezet feladatellátását befolyásolja és elengedhetetlen a magas biztonsági előírások teljesítésénél. A kívánt biztonsági szint elérése szervezetenként eltérő, külső recept nem létezi, ezért minden helyzetértékelés, kockázatelemzés és intézkedés egyedi, csak az adott szervezetre vonatkoztatható. Az emberi tévedés széles körű, nagyon sokféle emberi viselkedést tartalmazhat, ezért meghatározására és részletezésére különböző osztályozási rendszereket fejlesztettek ki, amelyeknek kifejtése jelen disszertációnak nem célja, ugyanakkor a hivatkozott kutatás alapján megállapítható, hogy az emberi tévedésből eredő hibák előfordulásának azonosítása segít csökkenteni az előfordulás

valószínűségét. James Reason „*human error*” modelljének közzétételében[369] kiemeli az aktív és a rejtett hibák jelentőségét. Rejtett hibák a következők lehetnek: gépek és berendezések rossz tervezése vagy kialakítása, képzés eredménytelensége, felügyelet hiányossága, kevésbé hatékony kommunikáció, valamint bizonytalanságok a szerepkörökben és a felelősségekben.[370] A rejtett hibák meghatározása az incidensek megelőzése szempontjából kulcsfontosságú tényező, mivel a megoldatlan, rejtett sérülékenység következménye a magasabb valószínűséggel bekövetkező incidensek, továbbá egy rejtett gyengeség gyakran befolyásol több lehetséges hibát, ezért eltávolítása az incidensek megelőzése szempontjából költséghatékony. Az információs rendszerhez kapcsolható „*human faktor*” (Health and safety guidance (HSG), Reducing error and influencing behaviour (1999.)) vizsgálatok és elemzések tehát nem hanyagolhatók el. Az elemzéshez hozzá tartozik az alacsony készség— és kompetenciaszint, egészségügyi állapot és alkalmasság, motiválatlanság és egyéb, a feladatelvégzésre ható emberi tényezők vizsgálata. A Munka Törvénykönyve[371] és a 33/1998. (VI. 24.) NM rendelet[372] szabályozza a munkavállaló egészségügyi alkalmassági vizsgálatára vonatkozó követelményeket, de a további, az alkalmazottat érintő emberi tényezők vizsgálata már a munkáltatói menedzser munkafolyamataiba épített feladatkör. A munkavállalót érintő stratégiai döntések során érvényesíteni kell a „*minden lánc olyan erős, mint a leggyengébb láncszeme*” elvet, amely következtében a kockázatkezelés „*humán faktor*” kockázatait is figyelembe kell venni. Az emberi hiba olyan cselekvés vagy döntés, amely egyrészt az elfogadott normától való eltérést jelent, és nemkívánatos eredményhez vezet, míg a szabálysértés egy szabálytól vagy eljárástól való akaratlan vagy szándékos eltérés, jogsértés. Az emberi hibákat két kategóriába sorolhatjuk: készség alapú mulasztás vagy tévesztés és a szabály vagy ismeret alapú hibázás. A mulasztás olyan jól ismert feladatoknál fordulhat elő, amelyeket tudatos odafigyelés nélkül is elvégezhetünk. A mulasztás az a hiba, amelyet még a legtapasztaltabb, jól képzett és motivált emberek is elkövethetnek. Jellemzően lehet gyakran kihagyott lépés egy javítási, karbantartási, kalibrálási vagy tesztelési feladatelvégzés során. A tévesztés egy feladat végrehajtásának kudarca, mint például: rossz komponens használata,

[369] Reason J (1990) Human Error, Cambridge University Press

[370] Health and safety guidance (HSG), Reducing error and influencing behaviour, United Kingdom for The Stationery Office (TSO), second edition 1999.

[371] 2012. évi I. törvény a munka törvénykönyvéről, VIII. fejezet, A munkaszerződés teljesítése, 29. Alapvető kötelezettségek, 51. § (4) bek., „*A munkáltató biztosítja az egészséget nem veszélyeztető és biztonságos munkavégzés követelményeit. A munkába lépést megelőzően és a munkaviszony fennállása alatt rendszeres időközönként köteles ingyenesen biztosítani a munkavállaló munkaköri alkalmassági vizsgálatát.”*

[372] 33/1998. (VI. 24.) NM rendelet a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről

működtetése, munkafolyamatok helytelen rendezése az adott eljárásban. Készség alapú hiba lehet különösen egy művelet túl korai vagy túl későn való végrehajtása, egy lépés vagy lépések sorozatának kihagyása a feladatból, egy művelet erőltetett vagy alacsony, az elvártnak nem megfelelő szintű végrehajtása, rosszirányú tevékenység, megfelelő tevékenység elvégzése rosszul megválasztott környezetben vagy rendszerben, és nem megfelelő ellenőrzés vagy teszt. Szabályalapú hibák elkövetésekor hajlamosak vagyunk ismert szabályokat vagy megoldásokat alkalmazni, még akkor is, ha nem ezek a legmegfelelőbbek vagy leghatékonyabbak, illetve már nem használatosak, csupán a legkényelmesebb módszerek. A szabálysértés a szabályoktól, eljárásoktól, utasításoktól és előírásoktól való bármilyen eltérés. A munkáltató által rögzített szabályok azok, amelyeket szükségesnek tartanak a biztonságos vagy hatékony munkavégzéshez, termeléshez, üzemeltetéséhez és karbantartásához. A szabályok megsértése lehet véletlen, nem szándékos vagy szándékos. A jogsértések típusai lehetnek például szándékos szabotázs vagy rongálás. A többségük a fennálló korlátok és elvárások ellen irányul. A jogsértéseket három kategóriába sorolják: gyakorlati, adott helyzetből fakadó és rendkívüli. A gyakorlati, jogsértő magatartás lehet automatikus vagy öntudatlan, ilyen esetben a szabálysértést az egyén vagy egyének felismerik, amennyiben az esetben felhívják a figyelmüket. A helyzetből fakadó jogsértés, visszaélés az alkalmazottak közvetlen munkaterületének vagy környezetének korlátai miatt következik be. Ide tartozik a munkaterület megváltozása, munkavégzésre kevésbé megfelelő környezet kialakítása és állapota, az elvárt, de ki nem fizetett túlóra, a személyzet száma vagy hiánya, a részleges felügyelet vagy ellenőrzés, az eszközök hiánya stb. A helyzetből fakadó jogsértés gyakran akkor fordul elő, amikor egy szabályt vagy utasítást lehetetlen vagy rendkívül nehéz megvalósítani az adott szituációban. A rendkívüli jogsértések általában ritkák, csak bizonyos körülmények között fordulnak elő, és gyakran egy nem várt esemény váltja ki. A jog- vagy szabálysértések kezelése állami hatáskör[373] [374]. A jogsértés olyan emberi magatartás, amely legalább egy jogi normával ellentétes és ezzel veszélyt jelent a társadalomra. A humán faktorral összefüggésben a jogsértés okai lehetnek az egyénben rejlő okok, jellembeli hiányosságok, ideológiai, munkahelyi vagy vallási feszültségek. Kutatásom során végzett statisztikai elemzések vizsgálata során megállapítottam, hogy a kiberbűnözők általában az információs rendszer gyengeségeit használják ki. Amennyiben gyengeségnek tekintjük a „humán faktor” bizonyos elemeit, akkor az olyan gyengeséget, mint a tudatlanságot vagy a hanyagságot sokkal könnyebb és olcsóbb

[373] 2012. évi C. tv. a Büntető törvénykönyvről
[374] 2012. évi II. tv. a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről

kihasználni, mint átjutni a kifinomult védelmi szoftvereken keresztül az adatbázis szerverig. Az emberi hiba, mint gyengeség csak abban az esetben okoz incidenst, ha a megvalósuláshoz megfelelő adottságok, környezeti tényezők és egy adott esemény, például támadási kísérlet együttesen jelen van.

5.3. A „*HUMÁN FAKTOR*” VIZSGÁLATA

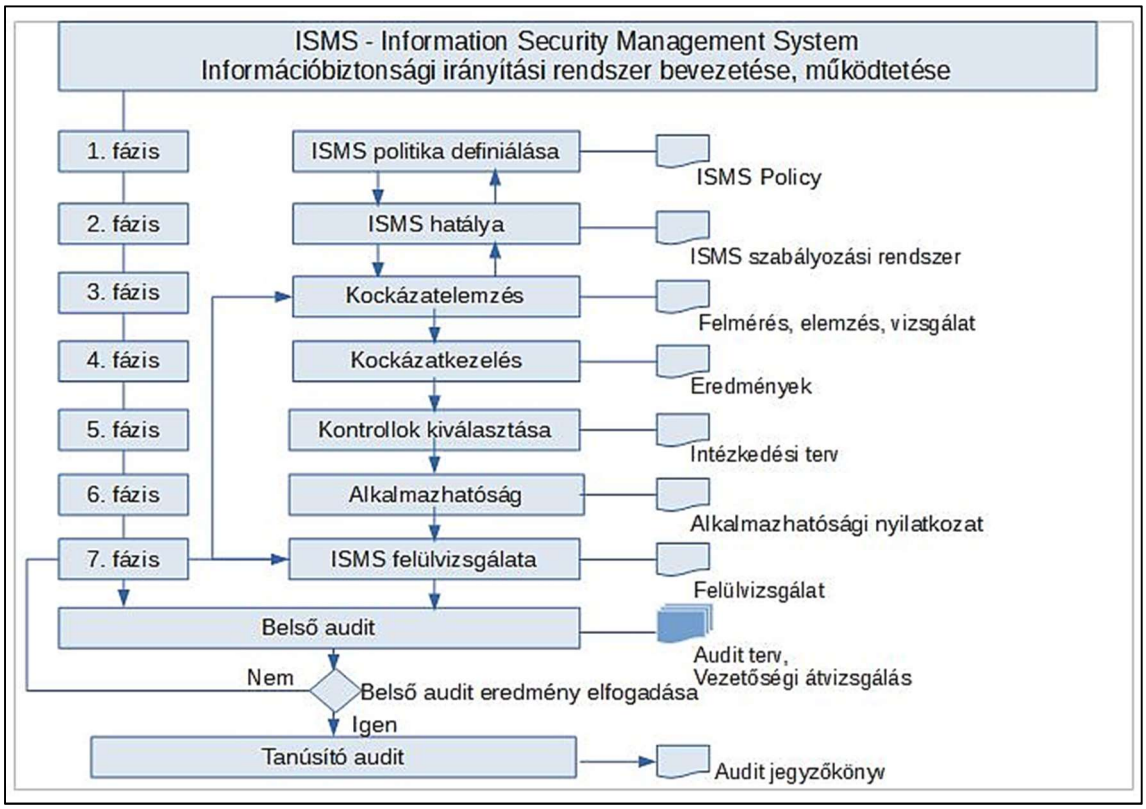
5.3.1. AZ ISO/IEC 27001 ISMS MÓDSZERTAN SZERINTI INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER BEVEZETÉSE ÉS A KOCKÁZATKEZELÉS EREDMÉNYEINEK BEMUTATÁSA

Nemzetközi, kanadai kutatás[375] szerint az adatmanipuláció (55%), a személyazonosság lopás (28%), a kártékony programok (53%), a csalás és a megtévesztés (46%) a legelterjedtebb információbiztonsági kockázati tényező, amelyet a Nemzeti Kibervédelmi Intézet statisztikai adatai (4. fejezet) és a hazai vonatkozású kutatásom eredménye (időszak: 2015-2020.) is megerősített. A vizsgálat során megállapítottam, hogy a személyes adatokra irányuló adatvédelmi jogsértések és illegális adatszerzésre irányuló információbiztonsági incidensek mértéke kiemelkedik a többi közül, ezért a legmagasabb kockázati tényező.[376] (Információbiztonsági kockázatok és fenyegetések kanadai felmérése, 2017.) A hazai vonatkozású kutatásom során egy olyan vállalkozás informatikai és információbiztonsági tevékenységét vizsgáltam, amely nemcsak információbiztonsági kutatásokat támogató szoftver fejlesztésével, hanem különböző informatikai rendszerek üzemeltetését is ellátta. A kutatás kezdeti szakaszában az ISMS bevezethetőségét, működtethetőségét és fenntarthatóságát, fejleszthetőségét és a szervezetre gyakorolt hatását vizsgáltam. Az alábbi statisztikai adatok a 10-20 főt foglalkoztató szervezet információbiztonsági felméréséből, az ISMS bevezetéséből és működtetéséből származnak. A kutatásom során alkalmaztam az ISO/IEC 27001 szabvány kritériumait és javasolt intézkedéseit, ami legfőképp a szabályozási rendszer felállítására, annak működtetésére, kockázatok (vagyonelem, sérülékenységek és fenyegetések) felmérésére és kezelésére (bekövetkezési valószínűség, hatáselemzés), intézkedések megvalósítására, valamint munkavállalók tudatosítására és belső audit végrehajtására fókuszált. Az ISMS

[375] Krisztina Győrffyné Holló, Adam Karisztl: Domino effect and other models in the it process, Gradus Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.
[376] Győrffyné Holló Krisztina, Információbiztonság, avagy megéri kockáztatni? In: Nagy, Bálint; Katona, József Az Informatika Korszerű Technikái Konferencia 2020 : Jövőformáló tudomány programfüzet és absztraktkötet Dunaújváros, 2020. november 9-10., Dunaújváros, DUE Press 2020. 48 p.p. 22

bevezethetőségének és fenntartásának sikere legfőképp a tervezési szakaszon múlik. Az információbiztonsági irányítási rendszer módszertanát maga az ISO/IEC 27001-es szabvány határozza meg, amely lényegét tekintve az IB szervező tevékenységének módszertana, az IB szervezési módszertan a szervezet tevékenységei, erőforrásai iránti bizalmasság, sértetlenség és rendelkezésre állás garantálására irányuló eljárási rend. A kutatás során az ISMS bevezetését kiterjesztettem az ISMS szabvány A mellékletében található kritériumok szerint a következő eljárásokra: vagyontárgyak biztonsága, emberi erőforrások biztonsága, fizikai és környezeti biztonság, a kommunikáció és üzemeltetés biztonsága, hozzáférés-ellenőrzés, fejlesztés, beszerzés, karbantartás, incidenskezelés, működés folytonosságának irányítása, kockázatkezelés. A sajátos szervezeti felépítés és működés szerint alakítottam ki a szabályozási környezetet, az ISMS politikát, az alkalmazhatósági területet, valamint a szervezeti biztonságra vonatkozó előírásokat. A megfelelés során figyelembe vettem a törvényi és szabványi előírásokat és ajánlásokat, valamint az ISO 27000-es szabványcsalád további szabványait, úgymint a mérésre, kockázatkezelésre, az auditálás követelményeire és az audit kontrollra, az üzletmenet folytonosságra (BCP), hálózatbiztonságra, alkalmazásbiztonságra, valamint az incidenskezelésre vonatkozó ajánlásokat. A szabályzatok és eljárások megalkotásánál különösen az ISO Guide 73[377], ISO 31000[378], GDPR, Infotv., IBtv. meghatározásait vettem alapul. A bevezetés során alkalmaztam a szabvány A mellékletének összes kritériumait, tehát a tanúsítás során sem zártam ki egy kritériumot sem. Az ISMS bevezetése és működtetése a PDCA elvek alapján történt, amelyet 7 fázisra osztottam. (16. ábra)

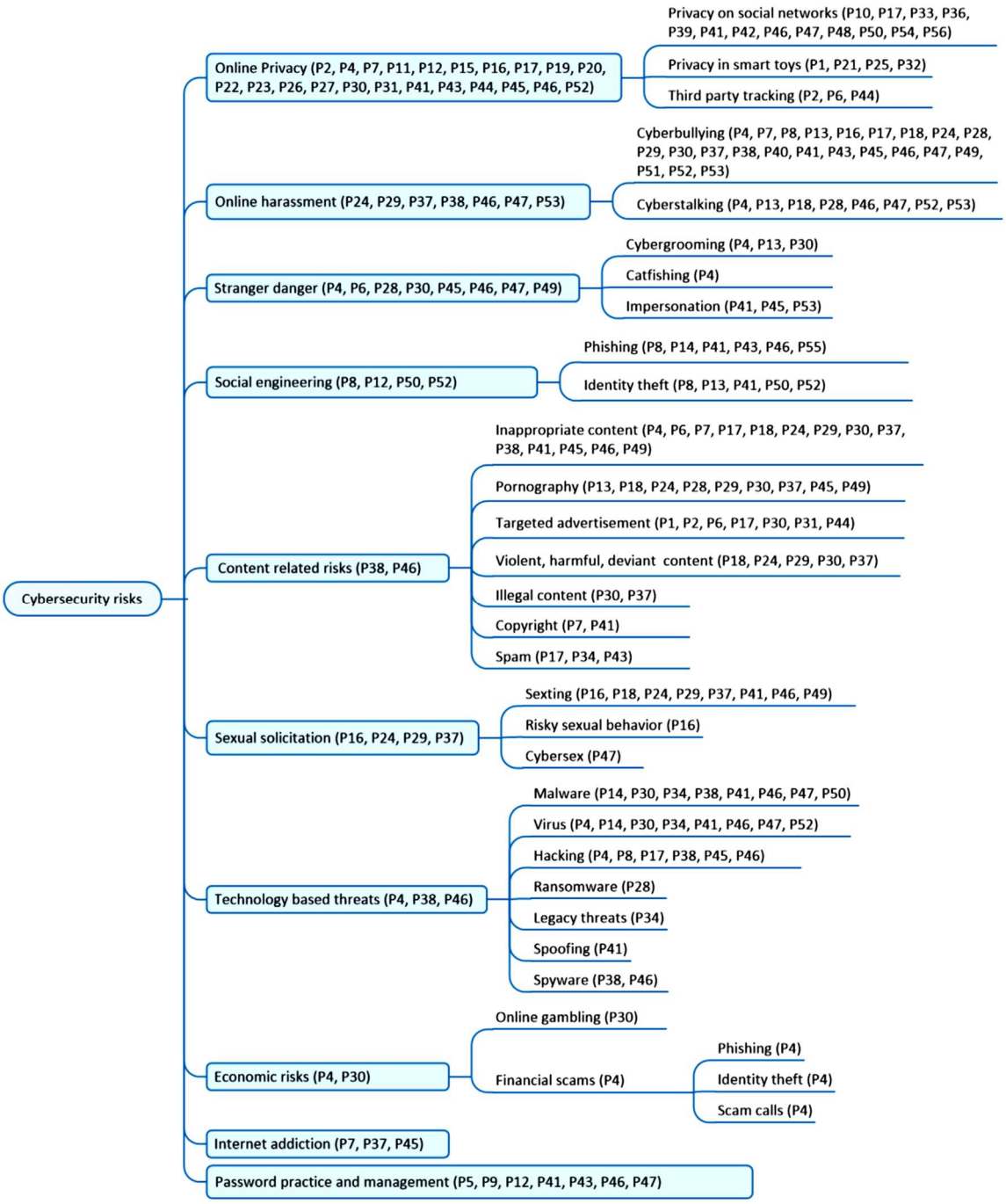
[377] ISO Guide 73, Risk management, Vocabulary
[378] ISO 31000, Terms and definitions



16. ábra, ISMS bevezetése és működtetése

saját kutatás során alkalmazott fázisok, saját szerkesztés

Az ISMS működtetésének jelentős részét a kockázatkezelés alkotta, úgymint releváns vagyonelem, sérülékenységek és fenyegetések felmérése, kockázat megállapítása, intézkedések meghatározása és végrehajtása, kockázatjavítás ellenőrzése.

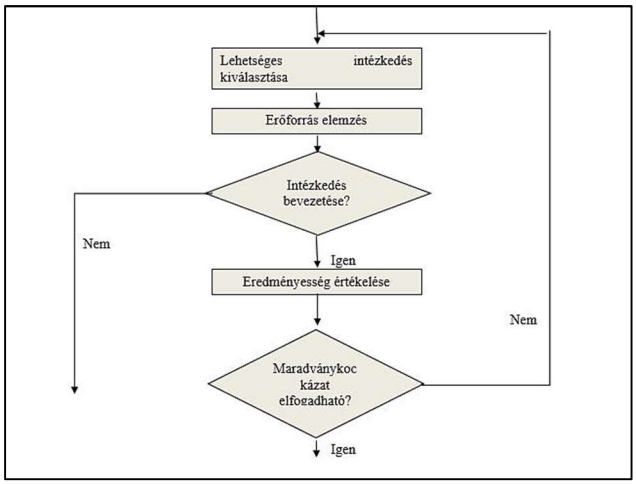


17. ábra, Gyermekeket érintő információbiztonsági kockázatok listája [379]

A kockázatkezelés során dokumentáltam a szervezetre vonatkozó működési hatáselemzést, a vagyonelemek kategorizálását, a vagyonelemek értékelését: fenyegetések, sebezhetőségek szempontjából, a lehetséges veszély hatásának mértékét és skáláját, a szolgáltatott, támogató folyamatok kritikusságát és osztályozását, a kockázatkezelés határértékét és az intézkedési

[379] Farzana Quayyum, Daniela S. Cruzes, Letizia Jaccheri, Cybersecurity awareness for children: A systematic literature review, International Journal of Child-Computer Interaction, Volume 30, 2021.

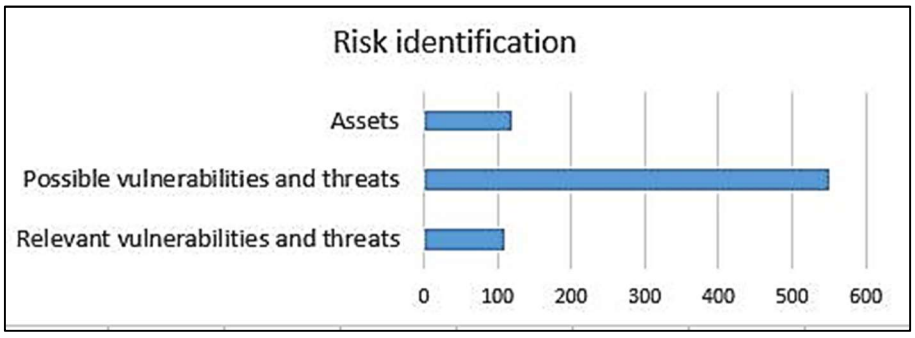
tervet. A kockázatkezelést szabályzatba foglalt előírás mentén hajtottam végre. A vagyonelemcsoportokat a hardver és egyéb fizikai eszközök, anyag, szoftver, hálózat, objektum (épület, biztonsági és egyéb zónák), papír és elektronikus alapú információ, valamint emberi erőforrás csoportjai szerint határoztam meg. A vagyontárgyakat a könnyebb azonosíthatóság miatt elsődleges és másodlagos vagyonelemcsoportra osztottam. Fenyegetés kategóriákat (36. ábra) különösen az szabályozás alapú (IB és ITB), admin és felhasználó, hacker, fizikai környezet, informatikai rendszer (OS), fejlesztői környezet, általános, valamint egyéb csoportba soroltam, például fizikai rongálás, alapvető szolgáltatás kimaradás okozta veszteség, természeti katasztrófa, ember vagy IT által okozott máshová nem besorolható. A fenyegetéseknél figyelembe vettem a szándékos és a véletlenszerű eseményeket. Tekintettel a fenyegetések eredetére és céljára, a kategóriák meghatározása évről évre módosul, valamint a vizsgált terület és új vagyonelem figyelembe vétele, a régiek inaktivitása szerint változik. Tehát a kategóriákat és a lehetséges kockázatokat mindig az aktuális állapotnak megfelelően kell meghatározni. A kockázatkezelési intézkedéseknél figyelembe vettem a szabályozás, szokás vagy gyakorlat, eljárások, vezetői előírások, szervezeti struktúra, szoftver vagy hardver megoldás, illetve fizikai védelmi szempontokat, és osztályoztam a megelőző, észlelő vagy elhárító típusú megoldások szerint. A kockázatkezelési intézkedéseknél figyelembe vettem az alábbi kockázatjavítási életciklus folyamatát.



18. ábra, Kockázatjavítási életciklus, saját kockázatkezelési kutatás alapján, 2015-2020., saját szerkesztés

A Kockázatjavítási terv tartalmazta a kezelendő kockázatok intézkedéseit, határidőt, felelősöket, a kiválasztás okát, prioritásokat, szükséges erőforrásokat, a teljesítménymérés módját, az auditálási és megfigyelési követelményeket. Az intézkedések során a legegyszerűbb

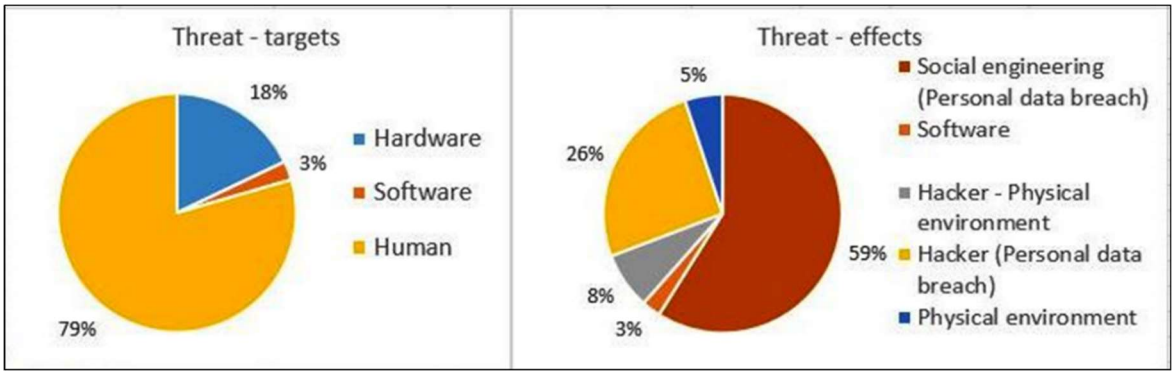
esetektől (mint például kábelrengeteg felszámolása) a legbonyolultabb feladatig (pl. felhasználói egyedi alkalmazásbeállítás webes felületen, profilozás nélkül – egyedi menüstruktúra, kedvenc lekérdezések, szűrők alkalmazása), vagy legnagyobb erőforrást igényló (szerverterem kialakítás, redundancia: vezetékek, elosztók, hálózat, áramellátás és UPS; tartalékolás, klímaberendezés, objektumvédelem) feladatelvégzésig, minden jelentős kockázatjavító feladatot számba kell venni, és megoldást kell találni a kezelésére. Minden esetben meghatároztam a maradványkockázatot. (18. ábra) A kockázatkezelést évente egy alkalommal vizsgáltam felül, az új munkavállalók IB képzését lehetőleg a munkába állást követő egy hónapon belül, a munkavállalói tréningeket és továbbképzéseket évente két alkalommal, a belső auditot szükség szerint évente egy vagy két alkalommal, a vezetői átvizsgálást és a tanúsító auditot évente egy alkalommal szerveztem. A munkavállalói képzések részét képezte a heti és havi rendszerességű, a szervezet vezetője által koordinált IT szakmai megbeszélések és tréningek. A vezetői átvizsgálás és a belső audit vizsgálat kiértékelésének részét képezte az IB terv-tény összefüggéseinek megállapítása. A kockázatkezelést az auditok (belső és tanúsító, illetve úgynevezett látogató) során teszteltük vagy felülvizsgáltuk. Az auditok (belső és tanúsító, illetve úgynevezett látogató) eredményét és javításra vonatkozó meghatározásait (megelőző és helyesbítő tevékenységek meghatározása; nem megfelelhetőségek; eltérések: észrevétel, enyhe, lényeges; megjegyzés) minden audit lefolytatása után, jegyzőkönyv formájában rögzítettük. Kutatásom során a fentiek alapján a következő információbiztonsági felmérési és statisztikai eredményeket állítottam össze.



19. ábra, Vagyonelem, sérülékenység és fenyegetés felmérése, saját információbiztonsági és kockázatkezelési kutatás alapján, 2015-2020.

A kutatás során 120 vagyonelemcsoportot, ennek 550 lehetséges sérülékenységét és fenyegetését vettem számításba, amelyből 110 releváns sérülékenység és fenyegetés bekövetkezési valószínűségét és az adott szervezetre vonatkozó lehetséges hatását vizsgáltam.

(19. ábra) A vizsgálat során az egyes esetekhez megállapítottam a lehetséges kockázat mértékét az 5.1.3.1 fejezetben ismertetett számítási mód alapján. Általánosságban megemlíthető, hogy a fenyegetések vizsgálatánál figyelembe kell venni a fenyegetettség orientációját, mert az esetenként eltérhet az elsődleges kár tárgyától. A fenyegetések elsődleges célpontja általában a személyes adatok megszerzése, másodlagos és akár valódi cél az illegális haszonszerzés, kutatási eredmények ellopása, ipari és gazdasági károkozás. A kockázatkezelés nem ér véget a kockázatok azonosításával és a kockázatszámítással. A kockázatok csökkentésének hatékony eszköze a kockázatfelmérés és a számítási módszer, amely segítségével a szervezet szempontjából jelentős információbiztonsági intézkedések megfogalmazhatók és végrehajthatók. A kutatás során bebizonyosodott, hogy a jelentős intézkedések végrehajtásával, a kockázatok évenkénti rendszerességű felmérésével és a belső auditok évenkénti lefolytatásával a magas kockázatú sérülékenységek és tevékenységek száma, valamint a reális fenyegetések bekövetkezési valószínűsége is csökkenthető.



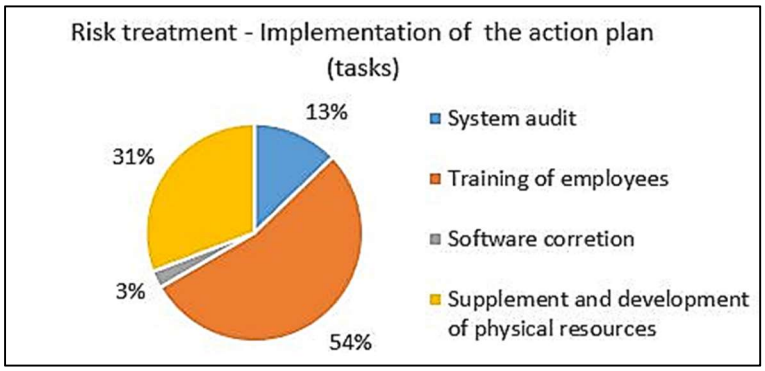
20. ábra, Fenyegetettség elemzés és lehetséges hatások felmérése saját információbiztonsági és kockázatkezelési kutatás alapján, 2020.[380]

A személyes adatokkal kapcsolatos incidensek (adathalászat, -vesztés, -lopás) aránya („*Social engineering*", 59%, hacker támadás 26%) azt mutatta meg, hogy ezen területeken a felügyeletet növelni kell. (20. ábra) A lehetséges incidens kategóriák esetében az ISO/IEC 27001 ISMS szabvány A melléklete szerint a legrelevánsabb csoport az adathordozók kezelése, a hozzáférés-felügyelet, titkosítás, biztonsági területek és fizikai beléptetési intézkedések, berendezések elhelyezése és védelme, üzemeltetés biztonsága, változásfelügyelet, védelem a rosszindulatú szoftverek ellen, mentés, naplózás és megfigyelés, kommunikáció biztonsága, a hálózatbiztonság, információátvitel, bizalmassági vagy titoktartási megállapodások, biztonság

[380] Krisztina Győrffyné Holló, Adam Karisztl: Domino effect and other models in the it process, Gradus Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

a fejlesztési és támogatási folyamatokban, tesztadatok védelme, valamint az információbiztonsági incidensek kezelése volt. Fenyegetés technikai kategóriái szerint az admin és felhasználó, hacker, fejlesztői környezet csoportjai bizonyultak a kockázati szempontból legrelevánsabb csoportkategóriának. A 2020-ban mért adatok szerint 110 lehetséges sérülékenység és fenyegetés közül optimális esetben 24 bekövetkezési valószínűsége alacsony (5-ös skála szerint 1), míg 15 közepes (5-ös skála szerint 3) értéket mutatott, hatáselemzés szempontjából 85 esetben magas (5-ös skála szerint 5), de alacsony bekövetkezési valószínűségű, míg 13 esetben közepes (5-ös skála szerint 3) értéket mutatott. Kockázati érték szempontjából 12 esetben (11%) kellett úgy dönteni, hogy a kockázatkezelés szempontjából kezelendő és intézkedés szükséges. Konkrét feladatmeghatározások között szerepelt a redundáns belső hálózat kialakítása, jogosultságok rendszeres ellenőrzése, redundáns adattárolás különböző földrajzi számú helyeken való kialakítása, szoftverek verziókezelése, szoftvernyilvántartás kezelése, biztonsági zóna megerősítése (biztonsági ajtók, ablakok kialakítása) vagy a kamerás megfigyelőrendszer figyelmeztető tábláinak elhelyezése és a videófelvételek tárolási korlátjának rendszeres ellenőrzése, valamint a mentések visszaállíthatóságának ellenőrzése. Bár a vizsgált szervezet esetében a szervezet üzleti adatainak biztonságos tárolását és védelmét külső szolgáltató biztosította, a helyi szintű szoftverfejlesztésekhez és külső partnerek felé nyújtott szolgáltatások teljesítéséhez saját, helyi szervertermet üzemeltettek. A helyi és a felhőben tárolt adatok esetében, az intranet és az internet hálózaton való eléréséhez is figyelembe kell venni a kommunikáció biztonságára vonatkozó kritériumokat. Az adathalászat esetében, az adatok megszerzéséhez sokszor a leggyengébb láncszemet célozzák meg, és a hacker által okozott adatvesztés az adathalászat következménye is lehet. Az adathalászatnál és a konfigurációs sérülékenységekből eredő adatvesztésnél a „*humán faktor*” vizsgálata elengedhetetlen. Kutatásom és a 2015-2020. években lefolytatott kockázatkezelési eljárások alapján megállapítottam, hogy a „*Social engineering*” és a sebezhetőségek kezelése, az emberi hibák bekövetkezésének megelőzése és a megelőzési módszerek alkalmazása 5-20%-kal csökkentheti az incidensek számát. A következő ábra megmutatja, hogy a kockázatkezelési eljárás során általam megfogalmazott intézkedések több, mint fele az információbiztonsági tudatosítás módszereket alkalmaz (54%), míg a fejlesztett szoftverek biztonsági korrekcióinak száma ennek töredéke volt.[381] (21. ábra)

[381] Győrffyné Holló Krisztina, Az információbiztonsági sebezhetőségek tényezőinek vizsgálata: A „humán faktor”, In: Váraljai, Mariann (szerk.) INFORMATIKA KORSZERŰ TECHNIKÁI KONFERENCIA 2021 „Jövőformáló tudomány” „Fenntarthatóság és digitalizáció” Dunaújváros 2021. november 9.: programfüzet és absztraktkötet, Dunaújváros, Magyarország : DUE Press (2021) 80 p. p. 40



21. ábra, Kockázatkezelési intézkedési tervben rögzített szükséges intézkedés típusok saját információbiztonsági és kockázatkezelési kutatás alapján, időszak: 2015-2020.

A kutatás során többféle információbiztonsági tudatosítási módszert alkalmaztam, különösen információbiztonsági oktatást, tréninget, egyénre szabott konzultációt és interaktív kommunikációt. Legtöbb esetben az egyénre szabott konzultáció bizonyult a legeredményesebbnek, mivel a munkavállalók korcsoportja, neme és szakképzettsége is eltérő volt. A belső audit alkalmával azt tapasztaltam, hogy a munkavállalók mindaddig betartják az előírásokat, amíg úgy érzik ellenőrzés alatt állnak. Amennyiben a tudatosítási és az ellenőrzési módszerek alkalmazása ritkábbá válik vagy elmarad, számos információbiztonsági kritérium, úgymint például a szabálykövetés, a napi mentés, a védett, elektronikus kommunikáció, a szerverterem szigorú védelme, a jelszópolicy jelentősége, ezáltal maga a biztonság is háttérbe szorul. A fő feladat, úgymint a szoftverfejlesztés vagy a rendszerüzemeltetés elsődleges prioritása nem azt jelenti, hogy a technológiai vagy adatvédelmi, illetve IB szabályokon lazítani lehet és figyelmen kívül hagyhatók az alapelvek. A kockázatkezelésnél vizsgált esetek, a NAIH által vizsgált utazási iroda adatvédelmi incidense is alátámasztotta a biztonságtudatos viselkedésre vonatkozó kutatási eredményeimet.

5.3.2. INCIDENSEK VIZSGÁLATA „*HUMAN FAKTOR*” SZEMPONTJÁBÓL

A „*humán faktor*” összefüggéseiben említett esetek (6.2.1 és a 4.3.1.1 számú fejezetek) incidenseit összehasonlítva az emberi tényezők jelentősen hozzájárultak az adatszivárgáshoz. Mindkét eset kapcsán megállapítható, jelentős személyes adat került nyilvánosan hozzáférhető állapotba, de a személyes adatokkal való visszaélés valós mértékére nem derült fény. Az érintett felek jelentős részének nem volt előzetes információja arról, hogy az adatkezelő mire használja az adatokat. Mindkét esetben megállapítható, hogy az incidenst az információbiztonsági

szabályok betartásával, több alkalommal meg lehetett volna akadályozni. A nem megfelelő adatkezelés és adatfeldolgozás során az emberi hibák eszkalálása egyre több problémát, végül incidenst okozott. Az incidensekhez kapcsolható általam vizsgált emberi hibákat, illetve azok elkerülését az következők szerint összegeztem. A törvényi rendelkezéseknek és a helyi szabályoknak való megfelelés céljából tájékoztatni kell az illetékes vezetőt és szükség esetén az érintett feleket a tervezett adattovábbítás ütemezéséről, a szükséges erőforrások igénybevételéről, az adattovábbítás kockázatairól, ezzel a cselekedettel el lehet kerülni az elfogadott normák megszegését és az esetleges jogsértéseket. Az adatmanipuláció előtt ellenőrizni kell a szerverkonfigurációt, és a tűzfalszabályokat. Az esetek túlnyomó többségében távoli eléréssel történik az adatkezelés vagy az adattovábbítás, ezért az adatmanipulációk megfelelő ismerettel való elvégezése elengedhetetlen. Adatmozgatás esetében célszerű az adatbázisszerkezet ismeretével is rendelkezni, mivel ennek hiányában az adatok sérülhetnek, adatvesztés is lehetséges. Az adatbáziskezelő rendszerek felépítése és parancsai eltérőek lehet egymástól, de megfelelő szakmai felkészültséggel az ismeretalapú hibázás a legkisebb mértékre csökkenthető. Az adat-, hálózat-, szoftveres és hardveres védelmi lehetőségek figyelmen kívül hagyása, a mulasztás egyik legnagyobb mértékű formája, mivel általában megállapítható, hogy a rendszerüzemeltető tudatában van a követendő szakmai és jogi szabályoknak és vélhetően szakmai felkészültsége is megfelelő, ezért a védelmi lehetőségek figyelmen kívül hagyása súlyos mulasztásnak minősül. Ezt enyhítheti a véletlen cselekedet, vagy a figyelmetlenséget, amelyet kiválthat más emberi tényező, mint például a fáradság vagy a betegség. Rendszerint a mulasztás felfedezésekor saját maga korrigálja a hibát. A fentiekben említett emberi hibákat felülmúlja a tudatos megtévesztés, amellyel elterelte a figyelmet a normák megszegéséről, a jogsértésről, az ismeret alapú hibázásról, vagy a mulasztásról. A rendszerüzemeltetők az incidens felfedezésekor teljesen szokásos informatikai eljárásként értékelték a tevékenységet, és az adatszivárgást teljes mértékben felróható a hacker rosszindulatú cselekedetének. Kutatásom során összehasonlítottam az emberi hibákat a 3.3.1.1 számú fejezetben közölt esettel valamint az 5.2.1 fejezetben közölt információbiztonsági eljárásokkal, amely szerint megállapítottam, hogy az emberi hibák jelentős része teljesül, a mulasztástól a jogsértésig, valamint az akaratlagos és a szándékos cselekedetig. Adatvédelmi szempontból az adatkezelő nem tett eleget a GDPR 25. cikk (1) és (2) bekezdésekben megfogalmazott rendelkezéseknek, a beépített és alapértelmezett adatvédelmi elveknek, és az adatfeldolgozó kiválasztásakor nem járt el elég körültekintően. Az adatkezelő olyan adatfeldolgozót bízott meg, aki súlyos, alapelvi szinten jogsértő cselekedetet hajtott végre, és adatkezelési, tervezési és végrehajtási

hiányosságokat okozott. A súlyos hiányosságok lehetővé tették, hogy az adatkezelés bizalmas jellegének sérülésével, magas kockázatú adatvédelmi és kibervédelmi incidens bekövetkezzen. Az adatfeldolgozó nem tett eleget a GDPR 32. cikk, az adatkezelés biztonságára vonatkozó rendelkezéseknek, mivel olyan módon kezelte a személyes adatokat tároló fájlszervert, hogy a fájlrendszerhez a sérülékenységet kihasználva, az interneten keresztül bárki hozzáférhetett. A sérülékenység miatt az adatok bizalmas jellege súlyosan sérült, ami lehetővé tette a magas kockázatú incidens bekövetkezését. Az adatfeldolgozó a jogsértést tovább súlyosbította azzal, hogy sem a felelős adatkezelő vezetőket, sem pedig az érintetteket nem tájékoztatta, az incidensről. Az adatfeldolgozó a GDPR 34. cikk (1) bekezdésében foglalt érintettek tájékoztatására vonatkozó előírásokat nem tartotta be, és ezzel megakadályozta, hogy az adatkezelő is eleget tegyen a GDPR vonatkozó előírásainak. A nevezett esetben az emberi mulasztás csak akkor válhat incidensé, ha adatlopás is történt. A 3, 4 és 5. fejezetekben vizsgált valós és lehetséges incidensek, illetve statisztikai adatok alapján megállapítottam, hogy a személyes adatokat érintő adatvesztés, illetve az incidensek eltitkolása kis- és nagyvállalatokat egyaránt érinti, arányaiban tekintve pedig az eltitkolások száma nagyvállalatoknál jelentősebb mértékű. Az incidensek eltitkolása drámai következményekkel járhat, ami jelentősen növeli az okozott kár mértékét. Ha az alkalmazottak, vagy az adatfeldolgozó eltitkolja az incidenst, annak oka kell, hogy legyen, és megelőzésére több módszert is alkalmazhatnak. Egyes esetekben a szigorúbb szabályozást, ellenőrzéseket vezethetnek be, valamint szankciókat alkalmazhatnak, más esetekben a tudatosítási módszereket helyezhetik előtérbe. Az incidensek, adatvédelmi jogsértések felméréseiből következtethető, hogy az adatfeldolgozók általában nem megfelelő módon osztanak meg tartalmakat, nem tartják be az információbiztonsági alapelveket. Előfordul, hogy az információbiztonsági politika nem fedheti le az összes kockázatot, másrészt sok esetben nem követik a szabályzatban foglalt előírásokat, ezért véleményem szerint egyértelmű megoldásokra van szükség, amelyekkel nagyobb hatékonysággal csökkenthő az adott kockázat mértéke, és megóvható az, ami számunkra a legfontosabb, a személyes adat, ezáltal növelhető a biztonságos munkavégzés szintje.

5.4. A „*HUMÁN FAKTORT*” BEFOLYÁSOLÓ EGYÉB TÉNYEZŐK

A „*humán faktor*” vizsgálatánál számba kell venni olyan környezeti összetevőket, amelyek csak közvetett módon éreztetik hatásukat. Befolyásoló tényező lehet munkahely vagy szervezeti és irányítási tényező. Munkahelyi tényező lehet például gépek és berendezések logikátlan tervezése, munkahelyi zavarok és munkafolyamat indokolatlan megszakítása, hiányos vagy

nem egyértelmű vezetői utasítások, rosszul karbantartott gépek és berendezések használata, nagy munkaterhelés, valamint zajos és kellemetlen munkakörülmények. Szervezeti és irányítási tényezők lehetnek, különösen a rossz munkatervezés, a szervezetlenség vagy a koncepció hiánya, a biztonsági rendszerek hiánya, a gyenge incidenskezelés és kockázatkezelés, az egyirányú kommunikáció, a koordináció és felelősség hiánya, a szegényes munkakörnyezeti adottságok (egészséges és biztonságos környezet hiányosságai), illetve a gazdasági és pénzügyi problémák. Az egyént befolyásoló tényezők, különöse az alacsony képzettségi és kompetenciaszint, a fáradtság, a motiválatlanság, az egészségügyi problémák. A fent említett egy-egy tényező nagyobb mértékű súlya a „*humán faktor*" egy-egy elemét olyannyira befolyásolhatja, hogy a következmény az adott rendszerre nézve fenyegetés vagy incidens, amely csak komolyabb költségráfordítással orvosolható. A véletlen vagy szándékos emberi hiba olyan cselekvés vagy döntés, amely az elfogadott normától való eltérést jelentette, és nemkívánatos eredményhez, általában pénzügyi illegális haszonszerzéshez, ipari vagy gazdasági kárhoz vezethet. Kutatási adataim rámutatnak arra, hogy a kezeletlen „*humán faktor*" eseteinek következménye a szervezet fenntartását, valamint működésének hatékonyságát negatív irányban befolyásolja. Több eset előfordulásakor a kártényezők hatása összeadódik és a következmény sokszor látványos, gazdasági vonatkozású.

5.5. A „*HUMAN-ERROR*" ÉS A MEGELŐZÉS MÓDSZEREI

5.5.1. A „*HUMAN-ERROR*" MODELL ALAPELVEI

Az emberi hiba eredetű gyengeségek, különösen a figyelmetlenség vagy az ismerethiány könnyen kihasználható, a hackerek által kedvelt biztonsági rések, mivel sokkal könnyebb és olcsóbb támadni, mint kihasználni a kifinomult védelmi konfigurációk csak részben ismert gyengeségeit. Ugyanakkor megfelelő módszerek segítségével az emberi hiba, javítható és az incidensek nagy része megelőzhető. A megelőzési eljárások kidolgozásához számos emberi tényezőt kell azonosítani. Az azonosításhoz segítséget nyújt különösen James Reason által meghatározott „*human-error*", a kutatásom során is felhasznált[382] svájci sajtmodelljéhez kapcsolódó 12 alapelv[383], amelyeket a továbbiakban foglalok össze. Az emberi tévedés nem erkölcsi kérdés, mivel az emberi természetéből adódó nem megfelelő tevékenység, döntés.(1)

[382] Krisztina Győrffyné Holló, Adam Karisztl: Domino effect and other models in the it process, Gradus Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.
[383] James Reason, Alan Hobbs, Managing Maintenance Error: A Practical Guide, 2003, James Reason's 12 Principles of Error Management

A hibák önmagukban nem rosszak, a kudarc nélkül nem tanulhatnánk és nem sajátíthatnánk el azon készségeket, amelyek nélkülözhetetlenek a biztonságos és hatékony munkavégzéshez.(2) Az ember megváltoztathatja az emberek munkakörülményeit. A különböző helyzetek különböző mértékűek, különböznek a nem kívánt cselekedetek is. A hibacsapdák azonosítása és jellemzőik felismerése elengedhetetlen előfeltétele a hatékony hibakezelésnek.(3) A legjobb emberek is elkövethetik a legrosszabb hibákat, tehát senki sem tévedhetetlen!(4) Az emberek nehezen kerülhetik el azokat a cselekedeteket, amelyeket nem is szándékoztak elkövetni. Az emberi hibák kárhoztatása érzelmileg kielégítő, de egyébként haszontalan és nem szabad összekeverni a hibáztatást az elszámoltathatósággal. Mindenkinek el kell számolnia saját hibáival és tudomásul kell vennie azok következményeit, továbbá törekednie kell arra, hogy elkerülje a megismétlődést.(5) A hibák olyan következmények, amelyek előzményekkel rendelkeznek. A hiba felfedezése az okok keresésének kezdete, nem pedig a vége. Csak a körülmények megértésével és a kiváltó okok kezelésével remélhetjük, hogy megakadályozzuk a megismétlődést.(6) Az ismétlődő hibatípusok javításának leghatékonyabb módja a megfelelő hibakezelési módszerek alkalmazása.(7) A biztonság szempontjából jelentős hibák a rendszer minden szintjén előfordulhatnak. Hibakezelési technikák akkor hatásosak, ha az egész rendszer területére kiterjesztjük.(8) A hibakezelés a kezelhető helyzetekről szól. Megfelelő módszer alkalmazásával a helyzetek és a rendszerek együttesen kezelhetők.(9) A megfelelő hibakezelési eljárás személyiségfejlesztő. A hibadetektálás készségének fejlesztése legalább olyan fontos, mint az emberek tudatosítása a hibák eredetében.(10) Nincs egyetlen legjobb módszer: Különböző típusú emberi tényezők problémáinak megoldása, a szervezet különböző szintjein, különböző irányítási és megoldási technikákat igényelnek.(11) A hatékony hibakezelés célja, a folyamatos megújítás és fejlesztés, nem pedig a helyi javítgatások sorozata.(12)

Kutatási adataim és munkahelyi tapasztalataim alapján véleményem szerint az emberi tévedésekre csökkentésére irányuló folyamat sokkal több, mint az egyén ellen indított fegyelmi eljárás precedens és annak üzenete. Számos olyan intézkedés létezik, amelyek hatékonyabb, ideértve a tervezést, a tudatosítási eljárásokat és a továbbképzést. A munkavállalói képzésekkel, tudatosítási módszerek alkalmazásával az incidensek jelentős része megelőzhető vagy hatékonyabban elhárítható, akár a tűz- és munkavédelmi oktatások alkalmazásának mintája alapján.

5.5.2. A TUDATOSÍTÁS JELENTŐSÉGE

A képzés és tudatosítás már az óvodákban (közlekedés szabályai) és az iskolákban elkezdődik, amely során nemcsak a való (a járda a gyalogosoké, az úttest az autóké), hanem a virtuális (smartjátékok, avatar) lehetőségekkel (közlekedés, játék és kapcsolatteremtés) és veszélyekkel (baleset, ismeretlen vagy fenyegető üzenetek, kéretlen reklámok) megismerkednek a gyermekek. Az alapok elsajátítása után a rendszeres információbiztonsági tudatosság fejlesztése nagyon fontos a középiskolákban és az egyetemeken egyaránt. A figyelemfelkeltés és az oktatás erősíti az alkalmazások biztonságos használatát, a szükséges biztonsági politika alkalmazását, az alapvető adatvédelmi szabályok megfelelő szintű betartását, ami különösen jelentős a felhasználók, rendszergazdák és adatkezelők közösségében. A tudatosítás további célja, a különböző felhasználók és szolgáltatók közötti biztonságos kommunikáció és együttműködés erősítése. Néhány, kutatásom során előtérbe kerülő statisztikai adatok alapján megállapítottam, hogy a kibertámadás célpontja lehet általában ipari, kereskedelmi vagy államigazgatási és közigazgatási szektor, ugyanakkor egyre több felsőoktatási intézmény vagy oktatói csoport esik a kiberbűnözők áldozatává. 2016-ban a Calgary Egyetemet ransomware támadás érte, amely során több, mint 15000 dollárt kellett fizetniük azért, hogy visszaszerezzék a hozzáférést a titkosított fájlokhoz. Az incidens következtében előírták az információbiztonsági figyelemfelkeltő tréningek megtartását, mivel az online bűnözők folyamatosan fejlődnek, újabb és újabb módszereket fejlesztenek ki a rendszer sebezhetőségeinek kihasználására és a felhasználók megtévesztésére, a rendszerek megtámadására. A gyerekek gyakorlatilag úgy születnek, hogy a kezükben van a technológia, de viszonylag kevés információjuk van az információbiztonságról.[384] Jacqueline Beauchere, a Microsoft Trustworthy Computing Group igazgatója szerint az iskolák felelőssége, hogy felkészítsék a gyerekeket arra, hogy okos, tehetséges, és átgondolt digitális állampolgárokká váljanak. A tanulóknak nemcsak elméleti szinten kell ismerniük a biztonságos internethasználati módszereket, hanem fel is kell készülniük arra, hogyan birkózzanak meg a digitális korszak iskolai vagy munkahelyi kihívásaival, illetve veszélyeivel. A tanároknak képzésre és támogatásra van szükségük ahhoz, hogy rendelkezzenek azokkal az információbiztonsági készségekkel, tudással és önbizalommal, hogy ezeket a témákat a tanulóknak is átadhassák. Létezik néhány megoldás informatikai biztonsági,

[384] 2011 State of Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey America's K–12 schools not preparing kids for digital age, study finds, https://www.prnewswire.com/news-releases/2011-state-of-cyberethics-cybersafety-and-cybersecurity-curriculum-in-the-us-survey-121240319.html, 2021. január 20.

információbiztonsági és adatvédelmi képzésre hallgatók, valamint alkalmazottak számára is, de az csekély. A felmérés is rámutat arra, hogy a tanulók számára a képzést be kell építeni az iskolarendszerbe, tehát a közoktatásba is, míg a munkavállaló számára a képességhez igazodó továbbképzést kell biztosítani.[385] Kockázatkezelési kutatásom (5.2 fejezet) során alkalmazott tudatosítási módszerek alkalmazásának eredményei is igazolják az előbbi megállapítást. A felmérés alapján megállapítottam, hogy minden korosztály és munkavállaló számára elérhetővé kell tenni az adatvédelmi és információbiztonsági alapelveket és aktuális információkat. Az információbiztonsági tudatosság fejlesztése elengedhetetlen az információbiztonsági tudatosság fejlesztési program keretében. A programban meghatározott felhasználói szintek kiterjesztése, de különös tekintettel az általános felhasználói szint esetében már nem kérdés, hanem szükséges. A szintek egyértelmű meghatározását és viszonyát, továbbá a szükséges tudásanyag meghatározását a kapcsolati modell segítheti.

5.6. AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG FEJLESZTÉSE

5.6.1. AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG MÉRÉSE

Kutatásom során megállapítottam, hogy a felhasználói, beleértve a rendszergazdai és rendszerfejlesztői információbiztonsági tudatosság állapotának és változásának mérése rendkívül összetett és bonyolult folyamat, amely során alkalmazhatunk kérdőív, interjú, mint önbevallási módszereket, gyakorlati teszteket vagy megfigyelési, automatikus számítógépes aktivitást mérő, adatgyűjtési eszközöket. Bármelyik módszert is használjuk, nemcsak a módszer kidolgozása és az adott szervezetre való igazítása rendkívül időigényes és komplex folyamat, hanem a kapott adat feldolgozása, kiértékelése is, hiszen figyelembe kell venni a szervezet sajátosságait, a munkahelyi körülményeket és az egyedi viselkedéstípusokat, és az adott szituációban releváns reakciókat. Az előbbiek figyelembevételével megállapítottam, hogy az információbiztonság-tudatosságra vonatkozó felmérés kivitelezése és értékelése is komplex tevékenység, amelynek eredményét torzíthatja egy-egy figyelembe nem vett tényező. Az információbiztonsági tudatosság felmérésre vonatkozó igény nem egyedi, számos publikáció foglalkozik ezzel a témával, amelyeket az ENISA szervezete is feldolgozott és tanulmányában publikált. Az ENISA felhasználva az Egyesült Királyság Nemzeti Kiberbiztonsági Központja (NCSC) által végzett kutatási eredményeket 2019-ben kiadta az információbiztonsági

[385] Krisztina Győrffyné Holló: The Human Factors of the IT Risk Management, Dunakavics, Dunaújvárosi Egyetem online folyóirata 2021. IX. évfolyam VII. szám, 47-61pp

viselkedés vonatkozásait tartalmazó kiberbiztonsági kultúra irányelveit.[386] Az Egyesült Királyság kutatása 688 publikáció eredményeire épült, és a módszerhez felhasználták a Google Scholar keresőrendszerét, ahol figyelembe vették az „*információs biztonság*", a „*biztonság*", a „*felmérés*", a „*kérdőív*" és a „*konstrukció*" keresési kulcsszavakat, valamint az publikálás idejét és a hivatkozások számát. A kutatási eredményeket kiegészítették a publikációk információival, mint például az absztrakt, a források, illetve a szerzői megjegyzések adataival, vagy a kutatás típusával (hallgatói vagy felhasználói vizsgálat) és a minta nagyságával (felhasznált adatok száma), illetve a cikk megadja-e a választ a kérdésekre, és ha igen, akkor azok milyen típusúak. A vizsgált publikációkban viselkedéstudományi módszereket is használtak olyan paraméterekkel, amelyek csak közvetett módon határozhatók meg, mint például az attitűd vagy a személyiségjegyek, és amelyekkel feltételezik, hogy befolyásolják az emberi magatartást, úgymint a biztonsági irányelveknek való megfelelést vagy a szabályok figyelmen kívül hagyását az információbiztonság területén. Az információbiztonsági magatartásokat vizsgáló szakirodalom átvizsgálása és a 478 releváns szakcikk minőségi szűrése után 47 tanulmány vizsgálatára összpontosítottak, amely szerint a módszertanok alkalmazása tekintetében a vizsgálatok túlnyomó többsége az információbiztonsági magatartások önbevallási mérőszámaira támaszkodott, ugyanakkor kreatívabb módszereket is alkalmaztak, mint például felhasználói jelszóerősség tesztelést, adathalász-szimulációt, biztonságtechnikai gyakorlatokat biztonsági adatmentésekre és naplózásra, valamint felhasználói adatgyűjtésre vonatkozóan. A kutatás értelmében, alátámasztva saját megállapításaimat, miszerint ezen populáris módszerek felhasználása potenciálisan problémás, mivel az önbevallás nem mindig korrelál a tényleges viselkedéssel. Szerintem ez az alapvető probléma a kérdőíves lakossági felmérés módszereknél, és annak valós eredményei, illetve következtetései tekintetében. Megállapítható továbbá, hogy a modellek hiányossága, mivel legfőképp háromféle modelltípus figyelhető meg, úgymint a védelmi motiváció elmélet, a tervezett viselkedési elmélet, valamint az általános elrettentés elmélet, amelynek alapja a kriminológiából származó modell. Az ENISA tanulmánya alapján, fenyegetettségi modelleknek csekély értékű előrejelző viselkedésük van, mivel a védekező cselekvési motivációra nézve gyenge, semleges vagy akár negatív hatása is lehet. Ez utóbbi megállapítással nem értek egyet, hiszen a jól megtervezett, valós fenyegetésekre és modellekre épített szimuláció eredményeit vizsgálva, az intézkedések végrehajtása kockázatcsökkentő tényező lehet (5.2.1 fejezet alapján). A „*Coping model*" használata több viselkedés-előrejelzés

[386] European Union Agency for Network and Information Security, (ENISA), Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, 2018. december

adatot eredményezhet. Tehát azok a módszerek, amelyeknek célja az, hogy javítsák például az adathalászatra vonatkozó megfelelő felhasználói reakció képességet, nagyobb valószínűséggel hoznak pozitív eredményeket, mint a fenyegetés hangsúlyozására épülő kampányok. A személyiség és demográfiai adatgyűjtési módszerek a felmérés alapján kevésbé voltak hasznosak, ezáltal kevésbé pontos vagy vegyes eredményeket értek el, így a sebezhetőség, az elfogadhatatlan biztonságtudatos viselkedés, attitűd szinte bármelyik korosztályban kiemelkedő értéket mutathat. A kvalitatív és vegyes módszerrel végzett vizsgálatok bizonyítékai tekintetében több olyan tanulmány készült, ahol a viselkedést befolyásoló tényezőket, a nem megfelelő magatartások okait először interjúk vagy megfigyelések alapján azonosították és a többfázisú vizsgálat első lépéseként rögzítették. Csupán egy olyan kutatást találtak, ahol az attitűd, a viselkedés és a motiváció közötti összefüggéseket vizsgálták. Ebben az esetben arra a következtetésre jutottak, hogy az alkalmazottakat információbiztonsági tudatosító programokkal és üzenetekkel kell megszólítani. Az interjú típusú vizsgálatok eredményeként megállapították, hogy a „*meg nem felelés*” leggyakoribb oka a túlzott munkaterhelés és a bonyolult biztonsági rendszer, ami blokkolta vagy megzavarta az emberek elsődleges feladatait és tevékenységeit, továbbá a munkavállalók jobban félnek a termelékenység következményeitől, mint attól, hogy ők okozzák az információbiztonsági incidenst. Az információbiztonsági politika figyelmen kívül hagyása miatt általában panaszkodnak, de a legtöbb szervezetben nem lépnek fel ellene addig, amíg az incidens be nem következik. A biztonsági kutatások rámutattak arra minden, nem biztonságos viselkedés esetén azonnal cselekedni kell, mivel a látens hibák egyesülnek, és incidensekhez vezetnek. A modern környezetben a szervezeteknek olyan alkalmazottakra van szükségük, akik felhatalmazással rendelkeznek és képesek fellépni a gyorsan fejlődő fenyegetésekkel szemben. A fenti elemzés alapján megállapítottam, hogy alapvető elvárás az, hogy az információbiztonsági tudatosság kialakításához azonosítani és elemezni kell a gyengeségeket vagy a problémák kiváltó okait. Az elemzés két alapvető részre osztható: a probléma és a kiváltó okok elemzésére, valamint a probléma tanulmányozására és a sikeres tevékenységek mérésére (Bow-tie modell, 4.2.2.1 fejezet). Itt is használható a többmódszeres megközelítés, mivel előfordulhat, hogy bizonyos kiváltó tényezők nem azonosíthatók az önbevallásos felmérések vagy a statisztikai adatok segítségével. Továbbá, egyes esettípusok könnyen mérhetők, mint például a kattintási arány (adathalászat, kéretlen levél - link, honlaplátogatás), ugyanakkor szerintem nem ez legmegfelelőbb mérőszám az információbiztonsági vagy digitális kultúra meghatározásához. Az ENISA riport, valamint dokumentumok és statisztikai adatok vizsgálata alapján

megállapítottam, hogy a formális értékelési és visszacsatolási mechanizmus minden információbiztonsági tudatosítási, képzési és oktatási program kritikus eleme. Az Ügynökség négy pontban foglalta össze megállapításait, amelyeket a dokumentumok vizsgálata szerint a következőkben összegzem. Ezen megállapításokat felhasználtam kutatásom során végzett kockázatkezelésnél és az intézkedések megfogalmazásánál is[387]. Az információbiztonság „*humán faktor*" értékelésében a mérőszámok jelentősek. Noha a számszerűsített viselkedési felméréseket gyakran tekintik a információbiztonság humán aspektussal rendelkező mérés és értékelés „*aranystandardjának*", ugyanakkor részletesebb eredményt kaphatunk, ha a különböző módszereket kombináljuk, tehát kvalitatív, kvantitatív és vegyes módszereket együttesen használjuk. Az ENISA a felmérés során megállapította, hogy a gyakorlatban a legtöbb mérőszám nem alkalmas a „*human faktor*" mérésére, vagy arra, hogy pontosabb információt adjon a viselkedés befolyásolásának módszereiről. Ahhoz, hogy az információbiztonsági intézkedés a digitális korszakában sikeres legyen, az iparágaknak a technológia- és folyamatközpontú szemléletről az emberközpontú szemléletre kell váltania, és alkalmaznia kell a viselkedéselméletek módszereit.(1) Az információbiztonság humán aspektusának tanulmányozására jelenleg használt modellek közül sok egyáltalán nem, vagy csak részben illeszkedik a tényleges viselkedéselemzéshez. Az attitűd-viselkedés modell (tervezett viselkedés elmélet), valamint ezen modell és a védelmi motivációs elmélet kombinációja a legelterjedtebb elméleti modell az információbiztonság tanulmányozására, de az eredményeket tekintve egyik sem ideális. A tervezett viselkedés elmélet esetében figyelmen kívül hagyja a tágabb értelemben vett tényezőket (szervezeti tényezőket), és feltételezi, hogy a megfelelés, különösen egy biztonsági politika, pozitív eredmény.(2) A kutatás alátámasztotta, hogy az információbiztonsági fenyegetésektől és következményektől való félelem nem hatékony eszköze a „*humán faktor*" megváltoztatásának.(3) A felmérések alapján megállapították, hogy a felhasználók által a fenyegetésekkel szembeni fellépés képesség és az információbiztonsági tudatos magatartás közti összefüggés csak részben kimutatható. Igazolható továbbá, hogy a felhasználók a fenyegetésekkel szembeni megküzdési készségeinek és információbiztonság-tudatosság növelése információbiztonsági szempontból pozitív irányú változásokhoz vezet. Az alkalmazotti motivációval pozitív irányú fejlődés várható, mivel megfelelő ösztönzési mechanizmussal a munkavállalók fokozottabban hozzájárulnak a szervezetet fenyegető problémák megelőzéséhez vagy elhárításához.(4)

[387] Krisztina Győrffyné Holló, Adam Karisztl: Domino effect and other models in the IT process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

Felméréseim szerint megállapítottam, hogy a 2018. előtt végzett kutatások nagyrészt a kibertámadások okozta hacker műveletek és rosszindulatú programok káros következményeire irányult. Az erre irányuló kutatások során megállapították, hogy a felderített öt legfontosabb kibertámadási fenyegetés közül ugyanakkor három emberi tényezőhöz kapcsolódott, úgymint a közösségi manipuláció adathalász e-mailekhez, az emberi hibákhoz és a szándékos visszaélésekhez.[388] 2015-ben a vizsgált adatvédelmi incidens 21,8%-a, 2016-ban pedig 15,8%-a volt adathalászat, hamisítás vagy manipuláció eredménye, míg 2017-ben az emberi hibák az adatvédelmi incidensek 19-36%-át tették ki országtól vagy régiótól függően.[389] (IBM, Ponemon Institute, Cost of Data Breach Study, Az adatvédelmi incidens kiváltó okainak százalékos aránya országonként és régiónként, 2017.) 2021. évben vizsgált incidensek többségét az adatszivárgás okozta, amely az emberi hiba okozta tevékenységre vezethető vissza. Az adatvédelmi jogsértésből eredő kár a felmérések alapján 4,24 millió dollár volt. (IBM, Ponemon Institute, Cost of Data Breach Study, 2021.) [390] Összehasonlítva a fenti statisztikai eredményeket, saját, 2015-2020. között végzett kutatásom szerint megállapítottam (5.2 fejezet), hogy amennyiben a rosszindulatú kódok és a szoftver hibák által okozott incidensek mögött, közvetett, kiváltó okként az emberi hibákat megvizsgáljuk, az emberi hiba az incidensek 36%-nál sokkal nagyobb arányú is lehet és elérheti a 80%-ot.[391] A kutatásom során bebizonyosodott, hogy az adatvesztési incidensek száma a tudatosítási módszerek alkalmazásával évenként 5-20%-kal csökkenthető, így optimális esetben akár pár év alatt minimálisra redukálható. Tehát az emberi hozzájárulás az információbiztonsági kockázatokhoz egyértelmű, ugyanakkor az információbiztonsági ismeretek átadása, a tudatosság növelése és az alkalmazottak magatartásának befolyásolása az IT kockázatok mérséklése érdekében nehézen megvalósítható feladat. Az emberi tényezők figyelmen kívül hagyása az információbiztonsági politikák és folyamatok kidolgozása és alkalmazása során, már a bevezetéskor kudarcra ítéli ezeket a tevékenységeket. Az alkalmazottak sokszor aktívan törekszenek arra, hogy az ún. kiskapuk kihasználásával megkerüljék a biztonsági irányelveket, amelyek megakadályozzák, hogy elvégezzék napi szintű feladataikat; mivel úgy érzik indokolatlan terhet ró rájuk, vagy nem értik, hogy miért kell prioritásként kezelni az előírásokat. Egy bizonyos küszöbön túl, a további biztonsági eljárások és követelmények betartatása ellenállást vagy megkerülési kísérletet

[388] M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, R. A. Khan, Healthcare Data Breaches: Insights and Implications, Healthcare 2020, 8(2), 133; https://doi.org/10.3390/healthcare8020133
[389] IBM, Ponemon Institute, Cost of Data Breach Study, 2017.
[390] IBM, Ponemon Institute, Cost of Data Breach Study, 2021.
[391] Krisztina Győrffyné Holló, Adam Karisztl: Domino effect and other models in the IT process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

eredményez. A tapasztalatok miatt hatékonyságra, rugalmasságra és alkalmazkodóképességre kell törekedni, amelyet az információbiztonsági kultúrának is támogatni kell. Az olyan innovációk, mint például a „*hozd magaddal eszközöd*" vagy a „*home office*" irányelv elfogadása és gyakorlása bizalmasságot és biztonsági gondolkodásmódot ébreszt az emberekben, egyben a rendelkezésre állás elvét is teljesítheti. Amennyiben az alkalmazottaknál elérjük a kívánt információbiztonsági képesség szintjét, élő tűzfalként gondoskodnak saját és általuk kezelt személyes és üzleti adatok megfelelő biztonságáról. A kezdeményezés ugyan még gyerekcipőben jár, de a következő fejezet rámutat arra, hogy ennek támogatása az Unió, az Országunk érdeke is, hiszen a felsorakoztatott tervek és lehetőségek segítik az információbiztonsági tudatosság magasabb szintre emelését.

5.6.2. AZ INFORMÁCIÓBIZTONSÁGI TUDATOSÍTÁS RENDSZERE ÉS FEJLESZTÉSI LEHETŐSÉGEK

Az utóbbi két évtizedben a digitális fejlődés a virtuális valóság, a mesterséges intelligencia, valamint a robotika nyújtotta lehetőségekkel gyorsabb változásokat eredményezett, amelyet ma már különösen az online oktatások, a reptéri arcfelismerés és COVID-19 állapotérzékelés során tapasztalhatunk. A digitális versenyképesség szintje egyre fontosabb feltétele a modern gazdaságoknak, az innovációnak és a gazdasági fejlődésnek. A digitális kompetencia, mint a fejlődés kulcsfontosságú összetevője, támogatása elengedhetetlen az egyéni és társadalmi fejlődés és a versenyképesség fenntartása érdekében. Ma már a digitális kompetencia azt jelenti, hogy aktívan, folyamatosan és a felelősség teljes tudatában, a társadalom minden szintjén, beleértve a politikai, a gazdasági, a kulturális és interkulturális tevékenységeket, ki tudjuk használni a virtuális világ adta előnyöket és lehetőségeket, miközben a potenciális kockázatokkal, fenyegetésekkel szembeni ellenálló képességünket fejlesztjük.[392] [393] Továbbá magában foglalja az információs műveltséget, az elvárt és megfelelő minőségű kommunikációt és az együttműködést, a médiaműveltséget, a digitális tartalomkészítést (beleértve a programozást), a biztonságtudatos tevékenységeket (beleértve a digitális és az információbiztonsággal kapcsolatos kompetenciákat), a szellemi tulajdonnal kapcsolatos kérdésekben való jártasságot, a problémamegoldást és a kritikai gondolkodást egyaránt. Az egyének képes legyenek arra, hogy a digitális technológiákat a készségek fejlesztésére

[392] Council of Europe (2018.), Reference Framework of Competences for Democratic Culture
[393] The Council of the European Union, Council Recommendation Of 22 May 2018 on key competences for lifelong learning, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0604(01)&rid=7, letöltés: 2021. december 18.

használják, valamint az információk kezelésére és védelmére, a tartalmat, az adatokat és digitális identitást felhasználják, hatékonyan kezeljék a szoftvereket, a digitális eszközöket, a mesterséges intelligenciát vagy a robotokat. A készségek közé tartozik a használat képessége, a hozzáférés, a digitális tartalmak szűrése, értékelése, létrehozása, programozása és megosztása. A digitális technológiákat alkalmazó magas színvonalú oktatás, beleértve a tanórán kívüli kompetenciafejlesztés, javítja az alapvető készségek szintjét. Véleményem szerint a digitális versenyképességhez, a digitális kompetencia fejlesztéséhez új tanulási módokat kell feltárni és alkalmazni, amelyet a DigCompEdu ajánlása is alátámaszt. A pedagógusok digitális kompetenciájának európai keretrendszere (DigCompEdu) egy tudományosan megalapozott keretrendszer. Általános referenciakeretet biztosít a pedagógus-specifikus digitális kompetenciák fejlesztésének támogatásához Európában. A DigCompEdu az oktatás minden szintjén oktatónak szól, a kisgyermekkortól a felsőoktatásig és a felnőttoktatásig, beleértve az általános és szakképzést, a speciális oktatást és a nem formális tanulási környezetet. A DigCompEdu 22 kompetenciát részletez hat területen, [394] ahol nem a technikai tudáson van a hangsúly. A keretrendszer inkább azt kívánja részletezni, hogy a digitális technológiák hogyan használhatók fel az oktatás és képzés javítására és fejlesztésére. Létfontosságú, hogy a pedagógusok rendelkezzenek azzal a digitális kompetenciával, amelyre minden polgárnak szüksége van ahhoz, hogy aktívan részt tudjon venni a digitális társadalomban. A polgárok európai digitális kompetenciakeretrendszere (DigComp) határozza meg ezeket a kompetenciákat. A DigComp a digitális kompetencia mérésének és tanúsításának széles körben elfogadott eszközévé vált, és Európa-szerte és azon kívül is a tanárképzés és a szakmai fejlődés alapjaként szolgál. A hat DigCompEdu terület[395] a pedagógusok szakmai tevékenységének különböző aspektusaira összpontosít, úgymint a szakmai elkötelezettségre[396], digitális forrásokra[397], a tanítás és tanulás jelentőségére[398], az értékelésre[399], a tanulók aktivitására[400], valamint a tanulók digitális kompetenciájának elősegítésére:[401]. A digitális kultúra elsajátítása, a digitális technológiák felelősségteljes használata egyben azt is jelenti, hogy a diákok képesek

[394] European Framework for the Digital Competence of Educators, DigCompEdu, https://ec.europa.eu/jrc/en/digcompedu, 2017.
[395] Krisztina Győrffyné Holló: The Human Factors of the IT Risk Management, Dunakavics, Dunaújvárosi Egyetem online folyóirata 2021. IX. évfolyam VII. szám, 47-61pp
[396] digitális technológiák használata kommunikációra, együttműködésre és szakmai fejlődésre
[397] digitális források beszerzése, létrehozása és megosztása
[398] digitális technológiák tanítási és tanulási használatának irányítása és összehangolása
[399] digitális technológiák és stratégiák használata az értékelés javítására
[400] digitális technológiák használata a befogadás, a személyre szabás és a tanulók aktivitásának fokozására
[401] lehetővé teszi a tanulók számára, hogy kreatívan és felelősségteljesen használják a digitális technológiákat az információ, a kommunikáció, a tartalomalkotás, a jólét és a problémamegoldás érdekében

az IT kockázatok kezelésére és a technológiák biztonságos használatára különböző területeken.[402] Az Európai Digitális Kompetencia Keretrendszer, más néven DigComp, eszközt kínál a polgárok digitális kompetenciájának fejlesztésére. A DigComp 2.0 nevű jelentés 21 kompetencia, a nyolc jártassági szint és a felhasználási példák a DigComp 2.1-ben találhatók. [403] [404] A digitális oktatási cselekvési tervről 2020. június 18. és szeptember 4. között lezajlott nyílt nyilvános konzultációra több mint 2700 hozzászólás érkezett. A hallgatókat megcélzó konzultáció középpontjában a COVID-19 válság során szerzett tanulási tapasztalatok álltak, amelynek információi szülőktől és gondozóktól, a szélesebb nyilvánosságtól, munkaadóktól és vállalatoktól, az oktatóktól és oktatási valamint képzési intézménytől származtak. Az Európai Bizottság 2020-ban elfogadta az első olyan digitális oktatási cselekvési tervet, amely az általános- és középiskolákra, valamint a felsőoktatásra egyaránt összpontosít. (Digitális képességek (EU), Digital Education Action Plan (2021-2027)) Az akciótervhez készített felmérés szerint a munkavállalók digitális készségek szintje átlagosan magasabb, mint a lakosság egészében, ugyanakkor az EU-ban a munkavállalók egyharmada nem rendelkezik alapvető digitális készségekkel. Ma már a legtöbb munkahelyen szükség digitális alapkészségekre, így a mezőgazdaság, egészségügy, építőipar ágazatokban egyaránt. Az OECD Felnőtt Készségek Felmérése (PIAAC - Programme for the International Assessment of Adult Competencies) szerint az Unióban a felnőtt lakosság több mint fele egyáltalán nem, vagy csak alap szintű digitális készséggel rendelkezik (e-mail írás vagy webböngészés). Tehát a munkavállalók fele ugyan minden nap használja az IT eszközöket a munkahelyén, anélkül, hogy meglenne a megfelelő készsége. A COVID-19 alatti távmunkavégzéssel a munkavállalók képesek voltak fejleszteni digitális képességüket (28,5%), de ez a lehetőség csak a számítógépes munkakörben dolgozókat érintette. A felsőfokú végzettséggel nem rendelkező és alacsonyabb képzettségű munkavállalók esetében csökken annak valószínűsége, hogy otthonról dolgoznak, tehát digitális képességüket sem tudták fejleszteni. [405] A világjárvány következtében egyre több

[402] Az IT eszközök és a digitális tartalom védelme, valamint a digitális környezetben jelentkező kockázatok és veszélyek, valamint az információbiztonsági intézkedések megértése, a személyes adatok és a magánélet védelme digitális környezetben, a személyes adatok felhasználásának és megosztásának megértése, miközben megvédheti magát és másokat az esetleges károktól, a digitális szolgáltatások adatvédelmi szabályzatának megértése és alkalmazása, az egészségügyi kockázatok elkerülése a digitális technológiák használata során, a digitális környezet lehetséges fenyegetésének megelőzése vagy felelősségteljes kezelése (például internetes zaklatás, kártékony kódok, vírusok és egyéb fenyegetések), a digitális technológiák alkalmazásának jótékony és káros hatásának felismerése és felelősségteljes használata.

[403] Európai Digitális Kompetencia Keretrendszer, European Digital Competence Framework, DigComp 2.1, https://ec.europa.eu/jrc/en/digcomp, 2017.

[404] A DigComp 2.1 EU-ajánlás alapján kidolgozott javaslat a tanulók digitáliskompetencia-szintjeinek meghatározásához és fejlesztéséhez, Digitális Pedagógiai Fejlesztések Munkacsoport, Oktatási Hivatal, 2021.

[405] Digital Education Action Plan (2021-2027), Resetting education and training for the digital age, https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en, letöltés: 2021. május 2.

munkaadó nyilatkozott arról, hogy beépíti a távmunkát a munkavégzési lehetőségek közé, továbbá a digitális fejlődés nagyobb adatgyűjtési, -feldolgozási és -elemzési kapacitást igényel, ami akár a gépi tanulással és a mesterséges intelligenciával együtt növelhetők az elemzési és digitális készségeket igénylő feladatok. Ez az igény magával vonja a korban és tudásban is többszintű digitális kompetenciafejlesztést, ami érinti az aktív és a leendő munkavállalókat, tehát a diákokat egyaránt. A felméréseken alapuló ENISA dokumentációja három területre terjedt ki, a digitális technológia jobb kihasználására a tanításban és a tanulásban, a digitális kompetenciák és készségek fejlesztésére, valamint az oktatás javítására a minőség tekintetében jobb adatelemzés és előrelátás révén. Az ENISA szabályokat is kidolgozott az információbiztonsági tudatosság fejlesztésére, amely szerint az EU tagországok részére kötelező az alapvető digitális készségek és kompetenciák fejlesztése kisgyermekkortól kezdve, a digitális kultúra fejlesztése, beleértve a dezinformáció elleni küzdelmet, a számítástechnikai oktatás, az adatintenzív technológiák fejlesztése, különösen a mesterséges intelligencia (AI) jó ismerete és megértése, a fejlett digitális készségek gondozása, amely több digitális szakembert eredményeznek, továbbá biztosítani kell a nemek közti egyenlő arányú részvételt a digitális tanulásban és karrierben. Európai vonatkozásban az EU kiberbiztonsági rendeletében (CSA, 2019.) kiemelték a információbiztonság fontos szerepét a figyelemfelkeltő és tudatosító kampányokban.[406] Az ENISA feladata, hogy előmozdítsa a magas szintű információbiztonsági tudatosságot, beleértve a kiberhigiéniát és a számítógépes műveltséget mind az állampolgárok, szervezetek és intézmények, valamint a vállalkozások körében.[407] Az Európai Kiberbiztonsági Hónap (ECSM - European Cybersecurity Month, október) keretében felhívja a nyilvánosság figyelmét a kiberbiztonsági kockázatokra, elősegíti az információbiztonsági tudatosságot és oktatást, valamint információbiztonsági útmutatást nyújt annak érdekében, hogy megteremtse a kibernetikailag biztonságosabb kultúrát. Az ENISA 2021. évi kutatása alapján készített jelentésben 3790 válaszadó által megadott adatok alapján, összegezték az EU kiberbiztonsági programjai által biztosított és preferált képzéstípusok arányát. A tanulmány során felmérték az egyes felnőttképzési, felsőoktatási kurzusokon belül a különböző biztonsági témákhoz rendelt kreditek összegét. Az összes olyan információbiztonsági program, a bachelor, master és egyéb posztgraduális képzés tekintetében, ahol adatokat szolgáltattak, megállapították, hogy a

[406] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), letöltés: 2019. november. 23.

[407] European Cybersecurity Month 2020 - Deployment Report, ENISA, https://www.enisa.europa.eu/publications/ecsm-deployment-report-2020, letöltés: 2021. április 24.

programok 48,45 %-a informatikai biztonság/mérnöki, 9,55 %-a jogi, etikai, adatvédelmi, kiberbűnözési, 12,11 %-a szervezési, kockázatkezelési, üzleti, 4,49 %-a szakmai gyakorlati, és 25,4 %-a egyéb képzés. (Információbiztonsági programok átlagos kiosztása, ENISA riport, 2021.[408]) Vizsgálatom szerint az adatok megmutatják, hogy az EU felsőoktatási intézményeinek információbiztonsági programjaiban több információbiztonsági mérnöki téma is jelen van. Ugyanakkor az alapképzések tekintetében az információbiztonsági és mérnöki témák csak 33,73%-ban vannak jelen, ehelyett jelentős az egyéb, más tartalmú képzés (42,92%). (Programok átlagos kiosztása, Bsc, ENISA riport, 2021.) A szervezési, kockázatkezelési, üzleti, valamint jogi, etikai, adatvédelmi és kiberbűnözési témák száma túl alacsony a munkaerőpiac (Cybersecurity Workforce Study, 2020.[409]) által megkövetelt készségekhez képest. Tehát a kockázatértékelés, -elemzés, -kezelés és -irányítás, valamint a kockázatkezelés és -megfelelőség a rangsorban csak a második és a negyedik helyet foglalja el a szakemberek érdeklődésére számot tartó legfontosabb információbiztonsági készségek között. A felsőoktatási intézmények programjainak implicit célja a diplomások felkészítése a kiberbiztonsági munkahelyekre. A munkaerőpiaci igényeknek való megfelelést többféle módon lehet biztosítani, egyrészt az adott szervezetben eltöltött gyakorlatok és értékes munkatapasztalatok alapján, továbbá az iparági oktatókkal folytatott programok biztosításával, kurzusokkal, amelyek a részvevőket professzionális biztonsági tanúsítvány megszerzésére készítik fel (pl. CISSP, CISM), vagy akkreditált szakképzéssel, amelyek közvetlenül támogatják az információbiztonsági vagy kiberbiztonsági karrier kialakítását. Az ENISA, Cybersecurity Higher Education Database (CyberHEAD) adatait tekintve az uniós programok mindössze 34%-a irányoz elő kötelező szakmai gyakorlatot a hallgatók számára. A szakmai gyakorlatok kialakítása kihívást jelenthet, a gyakorlati lehetőségek hiánya pedig negatívan befolyásolhatja a diplomások készségeit, és megnehezítheti a megfelelő állás elérését. Az iparral való együttműködés támogatására a kiberbiztonsági ágazatban, a programok 75%-ában volt jelen, ami jelentős nagyságúnak mondható, ugyanakkor nem találtam adatot arra vonatkozóan, hogy a leendő szakemberek milyen mértékben vesznek részt az ipar által biztosított programokon. (Hogyan készítik fel a programok a hallgatókat a munkaerőpiaci megfelelésre, ENISA riport, 2021.) Szakmai továbbképzés és minősítés tekintetében a képzések 23%-a készíti fel a szakembereket nemzetközi tanúsítvány (ISO 27001, CEH, CISM, CCNA Security, CySA+, CISSP és CompTIA Security+) megszerzésére, ami nagyon alacsony

[408] ENISA, Addressing Skills Shortage and Gap Through Higher Education, riport, 2021.
[409] (ISC)², Cybersecurity Workforce Study, 2020. https://www.isc2.org/Research/Workforce-Study, letöltés: 2021. december 18.

aránynak számít. A rangsorban az ISO/IEC 27001 szabvány tanúsítás a legnépszerűbb, amelyet a CEH és a CISM követ. Az információbiztonsági szakemberek számát figyelembe véve, a nemek tekintetében az arány 80% férfi és 20% nő, diplomás végzettségűek számát pedig az ENISA 2021. évi riportjának információbiztonsági diploma ábrája mutatja. Sajnálatos módon nem minden európai ország segítette adataival az elemzést, ezért némiképp hiányosnak tekinthető, ezáltal az erre épített következtetéseim vélelmezett információkat tartalmaznak. Az ENISA felmérése alapján az ügynökség az következő szabályokat fogalmazta meg. Növelni kell a felhasználói információbiztonsági tudatosságot mind a lakosság, mind pedig az alap- és középfokú oktatás körében. E tekintetben szerintem megoldás lehet az információbiztonsági ismeretek hiányosságainak azonosítása, a figyelemfelkeltés, illetve az alapvető ismeretek fejlesztése vagy megerősítése, esettanulmányok játékos feldolgozása és a játékos tesztek. Véleményem szerint, célcsoport tekintetében a munkavállalókat, az általános- és középiskolás diákokat is meg kell célozni, különös tekintettel a pedagógusok és egyetemi oktatók körére. Természetesen az utóbbi munkavállalói csoportok támogatása elengedhetetlen. A célcsoportok meghatározásának alapja információbiztonság-tudatosságnövelési program elmélete[410]. Támogatni kell a képzéseket az információbiztonság erősítése céljából a felsőoktatásban is, mivel ösztönözni kell a kiberbiztonsági együttműködést az akadémiai és az ipari szektor között, ami elsődlegesen az információbiztonsági képzések az üzleti igényekkel történő összehangolását jelenti. Továbbá támogatni kell a kiberbiztonsági gyakorlatokat a szimulációs és az éles akció során, verseny és ipari környezetben egyaránt. Az ENISA által támogatott információbiztonsági ismeretek hiányosságainak pótlására irányuló kezdeményezések többsége figyelemfelkeltő esemény volt, amely során a digitális készségeket beépítették az alap- és középfokú oktatásba. A kezdeményezés célja, hogy ne csak a fiatalabb generáció kiberképességeit javítsák, hanem az információbiztonsági tudatosságot is elősegítsék. Például Csehország esetében az „Oktatás és tudatosság” címmel, hangsúlyozták a kiberbiztonsági készségek fejlesztését és a lakosság oktatásának szükségességét. A fejlettebb európai országok az információbiztonsági oktatást már az óvodában elkezdik, aminek célja a digitális technológiák biztonságos használatának megtanítása. A Nemzeti Kiber- és Információbiztonsági Ügynökség igyekezett biztosítani, az általános- és középiskolai szinten is cél legyen a megfelelő információbiztonságikészségek kialakítása. Görögország különös

[410] Mádi-Nátor Anett, Kardos Zoltán, Nemzeti Közszolgálati Egyetem, Mádi-Nátor Anett, Kardos Zoltán, Információbiztonság-tudatosság gyakorlat, Nemzeti Közszolgálati Egyetem, https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsag-tudatossag-gyakorlat.original.pdf, letöltés: 2022. január 18.

hangsúlyt fektet a kapacitásépítésre és az információbiztonsági készségek fejlesztésére, úgymint a fiatalabb nemzedék megfelelő ösztönzőinek megteremtése annak érdekében, hogy megismertesse őket a kiberbiztonsággal, és rávegye őket arra, hogy tanulmányi vagy szakosodási tárgyként tekintsenek erre a szakterületre. Támogatni kell az új, közös kezdeményezéseket az információbiztonsági készségek hiányának és hiányosságainak kezelésére. Mivel sok tagállamban felmerült az információbiztonsági készségek hiánya és hiányossága, szükséges a közös kezdeményezés elindítása, amely előnyös megoldás lehet az erőforrások hiányára, illetve a meglévők összevonására. Együttműködésekre számítanak különösen a kiberbiztonsággal kapcsolatos tananyagok kidolgozása, a közös, figyelemfelkeltő kampányok kiadása terén. A fenti elemzés alapján megállapítottam, hogy azokban a tagállamokban, ahol a végzett és alkalmazott szakemberek száma az Uniós átlagot nem éri el, feltétlenül javasolt az Unió által rendelkezésre bocsájtott erőforrások kihasználása. A CyberHEAD egyedülálló adatbázist biztosít az EU és az EFTA országok információbiztonsági kurzusairól. A tanulmány alapján vizsgálatot végeztem a magyarországi egyetemek tekintetében is, amely szerint megállapítottam, hogy Magyarországon az Óbudai Egyetemen akkreditáció alatt áll kiberbiztonsági mérnök BSc szak, a Nemzeti Közszolgálati Egyetemen kiberbiztonsági MA, illetve posztgraduális, az Eötvös Lóránd Tudományegyetemen pedig kiberbiztonsági MSc képzés található. Néhány egyetem, mint például a Budapesti Műszaki és Gazdaságtudományi Egyetem, valamint a Budapesti Corvinus Egyetem információbiztonsági szakterületen néhány kurzus keretben elsajátíthatják a hallgatók a kiberbiztonság és –védelem néhány tananyagát. Saját tapasztalatom szerint a diákok számára az informatikai oktatás keretébe, heti rendszerességgel be lehet építeni az informatikai technológiai, adatvédelmi és információbiztonsági tananyagokat. Ma már az ötödikes diák is képes arra, hogy tudását és gondolatait szövegszerkesztő vagy előadástervező segítségével közvetítse az osztálya és tanára részére. Ezeket a prezentációkat nemcsak órai beszámolóhoz, hanem versenyre is elkészítik a diákok. Tehát, ma már egy tíz-tizenkét éves gyermek számára az alapvető digitális programok elsajátítása nem jelent problémát. A COVID-19 adta online oktatások segítették ezen kompetenciák kifejlesztését, mert a szükséges távolságtartás helyzete rákényszerítette a szülőt, diákot és a pedagógusokat egyarán a különböző informatikai megoldások kipróbálására és használatára. Természetesen minden bevezetési időszak nehéz, mert új kihívások elé állított mindenkit, de a világjárványból adódó szituációk megoldása elengedhetetlenné vált. Kezdetben a gyors alkalmazkodás és a hiányzó programleírás miatt, sok esetben a diákok egymást tanították a különböző elektronikus programok használatát. A digitális oktatás során a

pedagógusok, mint koordináló személyek kulcsszerepet játszottak. A digitális oktatás egyik legfontosabb eleme a személyes adatok védelme. A tudás elsajátítása és a digitális jogok és felelősségek megértése, a diákok személyes adatainak felhasználása és a biztonságtudatosság fejlesztése, a kockázatok tudatosítása, a digitális környezetben való magabiztos közlekedés tanítása, az adatvédelmi alapelvek betartása alapvető célkitűzés volt, amelyet már korábban (2013., 2017.) a NAIH több tájékoztató és kiadvány közreadásával, valamint a diákok számára készített, hivatalos iskolai programok és pedagógusok képzése során használható, kifejezetten adatvédelemmel kapcsolatos oktatási anyagokkal is támogatott.[411] A kiadványok tartalmazzák a magánszféra és a személyes adatok védelmére, informatikai technikai szempontokra, szabályozásra vonatkozó célkitűzéseket, szükséges ismereteket és készségeket. A kiadványok az esetek bemutatása által kiemelik azon jelentősebb területeket, amelyekre az általános, középfokú informatika tantárgy oktatása során fokuszálni kellene.[412] Az informatika világa technikai lehetőségeket nyújt a szórakozásra, a tanulásra és a munkavégzésre, és az oktatások során, ugyanakkor véleményem szerint, nemcsak a lehetőségeket, hanem a kihívásokat, az adatvédelmi alapelveket, az incidenseket és azok megelőzésének módszereit, is be kell mutatni, ahhoz, hogy a diák megfelelő képet kapjon a virtuális világról. Ahogy a kisgyermeknek meg kell mutatni, mi a különbség a tankos online játék és a neten található háborús képek, videók között, úgy a fiatalokat is tájékoztatni kell az internetes zaklatás formáiról, és a megelőzési módszerekről. A gyermekek önmaguktól is rátalálnak a veszélyes forrásokra, tehát a felnőttek, legyen az szülő vagy pedagógus, kötelessége megmutatni a digitális világ árnyoldalát és az incidensek elkerülési vagy az elleni, védekezési megoldásokat. A NAIH 2017. évi felmérése alapján már az óvodás gyermekek 30%-nak, illetve általános iskolás, alsó tagozatos gyermekek több, mint 60%-nak volt saját digitális eszköze.[413] Azóta ez az arány csak nőtt. A saját digitális eszköz használata ugyanakkor nem jelenti a digitális kompetencia automatikus kialakulását is. A NAIH felmérése szerint a gyermekeket a digitális eszköz használatát általában a szülő vagy a testvér, de több esetben senki sem tanította meg, illetve autodidakta módon tanulta. Az internethez a gyermekek 2/3-ának volt hozzáférése. A felmérés rávilágít a 2017. évi adatvédelmi alapelv és technikai tudás és kompetenciahiányosságokra. Az informatika több,

[411] ADATVÉDELMI BIZTOSOK NEMZETKÖZI KONFERENCIÁJA, A személyes adatok védelmének kompetencia keretrendszere diákok számára, Segédlet pedagógusok részére, 2016., https://www.naih.hu/files/kompetencia-keret-diakoknak.pdf, letöltés: 2022. január 16.

[412] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Kulcs a Net világához! A NAIH tanulmánya a gyermekek biztonságos és jogtudatos internethasználatáról https://www.naih.hu/files/2013-projektfuzet-internet.pdf, 2013., letöltés: 2021. április 27.

[413] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Kulcsocska a net világához, https://naih.hu/files/kulcsocska-a-net-vilagahoz-2018-01-29.pdf, 2017.

mint néhány táblázatkezelési, bemutatókészítési, illetve szövegszerkesztési lehetőség. A gyermekeket ért incidensek (provokáció, zaklatás, internetes pedofília, behálózás) növekedése is azt mutatja, hogy az évi 3-4 alkalom kevés az információbiztonságra, ehelyett kezdetben játékos, szituációs és vicces esetekkel kell az életükbe csempészni, majd érettségüknek megfelelően komolyabb esetvizsgálatokkal és védelmi lehetőségekkel kell erősíteni az információbiztonsági készségek kialakulását, a biztonságtudatos magatartás megszilárdulását. Magyarországon az Oktatási Hivatal által 2021-ben kiadott DigComp javaslata szerint a 21 kompetencia és a négy szint (alap-, közép-, felső- és szakértői) leírás alapján kell kidolgozni és bevezetni, valamint alkalmazni a digitális képességek fejlesztését.[414] A javaslat az információkezelés, kommunikációs, tartalomszerkesztés, biztonságtudatosság és problémamegoldás digitális kompetenciákra fejlesztésére összpontosít. A digitális kultúra (9-10. évfolyamon: 102, míg 11. évfolyamon 68 órában) középiskolai tananyagban a diákok évfolyamonként 3-4 óraszámban, tehát a három év alatt összesen 10 óraszámban, az információs társadalom és e-világ témakörén belül sajátíthatják el az adatvédelem és információbiztonsági fogalmakat és ismereteket.

5.6.3. AZ INFORMÁCIÓBIZTONSÁGI TUDATOSÍTÁS FEJLESZTÉSÉRE VONATKOZÓ JAVASLATOK

Kutatásom alapján megállapítottam, hogy a rendszerüzemeltetők és a számítógéppel dolgozó felhasználók számára is új helyzetet teremtett a COVID-19 világjárvány, ami miatt egyre gyakoribb az otthoni munkavégzés, éppen ezért javasolt az otthoni munkavállalói feladatok körültekintőbb elvégzése. A fenti adatok alapján egyértelműen megállapítható, hogy a hacker próbálkozások nagy részének célpontja a gyenge láncszem, különösen a felhasználó, aki gyanútlansága vagy figyelmetlensége okán áldozattá válik és ipari vagy személyes, illetve banki adatokat szolgáltat ki sok esetben anélkül, hogy arról tudomása volna.[415] Az úgynevezett „*home office*" feladatait segíti a globálisan meghatározott, és speciális, helyi szintű előírásokkal kiegészített információbiztonsági útmutató. Az útmutatók alkalmazásával csökkenthető a hackerek által okozott incidensek száma. A következő fejezetekben a hatóságok által kiadott ajánlásokat, valamint a saját kutatásom során szerzett tapasztalataimnak

[414] Oktatási Hivatal, NAT, Digitális kultúra tantárgy, 2020.
[415] Krisztina Győrffy , Ferenc Leitold , Anthony Arrott: Individual awareness of cyber-security vulnerability – Citizen and public servant, CEE eDem and eGov Days 2017: Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?, Budapest

megfelelően összegeztem azokat az információbiztonsági javaslatokat, amelyeket az otthoni munkavégzés során is követni kell.

5.6.3.1. AZ ADATVÉDELMI MUNKACSOPORT HÉT LÉPÉSBŐL ÁLLÓ MÓDSZERTANA

Nemcsak információbiztonsági útmutatók, hanem adatvédelmi eljárással kapcsolatos módszerek segíthetik az adatkezelők munkáját. Az Adatvédelmi Munkacsoport hét lépésből álló módszertant ajánl a 06/2014. számú véleményében[416] az adatkezelőknek. A hivatkozott lépések lényegében konkrét utasítás sorozat, amely segítséget nyújt az adatkezelőnek abban, hogy az érintett által rábízott személyes adatokkal jogszerűen, az érintett érdekeit figyelembe véve, körültekintően járjon el. Egyes nagyvállalati és intézményi szférában teljesen elfogadott a folyamatok meghatározása és az eljárásrendek kidolgozása minden munkafolyamat tekintetében kötelező. Az alkalmazottak az eljárás szabályaitól csak különleges esetben térhetnek el, az egyedi munkafolyamat megvalósítását indokolni kell. Az eljárásrendeket nemcsak a folyamatos termelés, a gazdaságosság vagy az üzletmenet-folytonosság irányelveinek figyelembevételével határozták meg, hanem a szabályok betartása információbiztonsági (tartalmazza a fizikai biztonságot is), biztonságtechnikai, tűz- és munkavédelmi szempontból is jelentős.

5.6.3.2. AZ EURÓPAI ADATVÉDELMI TESTÜLET IRÁNYMUTATÁSA

A jogsértésnek számos jelentős káros hatása lehet és következménye lehet fizikai, anyagi vagy nem vagyoni kár is. A GDPR útmutatása szerint az okozott kár magában foglalhatja az irányítás elvesztését is személyes adatok felett, a jogok korlátozását, továbbá a személyazonosság-lopást vagy csalást, anyagi veszteséget, az álnevek jogosulatlan megfordítását, a jó hírnév megsértését és a bizalmas adatok elvesztését, bármilyen jelentős gazdasági, illetve társadalmi hátrányt. Az adatkezelő egyik legfontosabb kötelezettsége a GDPR és az Infotv. szabályainak megfelelő

[416] 29. cikk szerinti Adatvédelmi Munkacsoport a 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról szóló 06/2014. számú vélemény, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf, letöltés: 2021. december 23.
1. lépés: Melyik a potenciálisan alkalmazható jogalap a 7. cikk a)–f) pontja közül?
2. lépés: Az érdek jogszerűségének vagy jogszerűtlenségének megállapítása.
3. lépés: Az adatfeldolgozás az érdek érvényesítéséhez való szükségességének megállapítása.
4. lépés: Ideiglenes egyensúly elérése annak mérlegelésével, hogy az adatkezelő érdekeivel szemben elsőbbséget élveznek-e az érintettek alapvető jogai vagy érdekei.
5. lépés: Végleges egyensúly elérése a kiegészítő biztosítékok figyelembevételével.
6. lépés: A megfelelés bizonyítása és az átláthatóság biztosítása.
7. lépés: Mi történik, ha az érintett él a tiltakozási jogával?

technikai és szervezési intézkedések megvalósítása.[417] Az adatszivárgás megelőzése eredményesebb és hatékonyabb, mint a következmények helyreállítása, amelynek egyes része visszafordíthatatlan. Az Európai Adatvédelmi Testület (European Data Protection Board, EDPD)[418] által 2021. december 14-én kiadott, 2021/01. 2.0 verziószámú, *Példák a személyes adatok megsértésére vonatkozóan* irányelv célja, hogy segítse az adatkezelőket az adatvédelmi incidensek kezelésében, és a kockázati tényezők vizsgálatára vonatkozó kockázatértékelés során. A figyelmeztetés az alábbi hat témára összpontosít, amelyek a CIA (bizalmasság-sértetlenség-rendelkezésre állás) információbiztonsági alapelvek meghatározásán, illetve megsértésén, valamint a GDPR által előírt adatkezelői és adatfeldolgozói kötelezettségek meghatározásán alapulnak[419]. A témák jelentőségét a napi életből vett incidensek bemutatásával és szakmai jellemzésével igazolták. Az iránymutatás kiemelt témái között szerepel a célkitűzések és CIA információbiztonsági fogalmak meghatározása, az adatkezelők általi, személyes adatokkal kapcsolatos jogsértésre vonatkozó dokumentálási, bejelentési és érintettel való tájékoztatási kötelezettségek összefoglalása, az adatvédelmi incidens kezelésére vonatkozó szükséges eljárások, az adatvédelmi képzés és tudatosítás a tréningek, kibertámadási trendek és biztonsági események jegyében, valamint az elszámoltathatósági elv és az adatvédelmi koncepció beépítése az adatvédelmi eljárásokba, adatkezelői „*Kézikönyv a személyes adatok megsértése kezeléséről*” című kiadvány összeállítása, ami lényegét tekintve forgatókönyv az adatfeldolgozásra és az incidenskezelésre. A témák között szerepel a Ransomware típusú támadás[420]. A Ransomware típusú incidensek elkerülésére, illetve kezelésére vonatkozó javaslat alapján szükséges a firmware, az operációs rendszer és az alkalmazás naprakészen tartása, biztonsági frissítése, naplózás, biztonsági javítások nyomkövetése (időbélyeg használata) a szervereken, a kliensgépeken, az aktív hálózati eszközökön (csomópontokon és végpontokon) egyaránt, a különböző funkciót betöltő alhálózatok szegmentálása, elszeparálása és a strukturált hálózat kialakítása, a naprakész, biztonságos és tesztelhető biztonsági mentési eljárás kidolgozása és megvalósítása, biztonsági másolatok az üzemeltetési területtől elkülönített tárolása, védelem kialakítása harmadik fél

[417] European Data Protection Board, Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021, Version 1.0, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf, letöltés: 2022. január 15.

[418] Európai Adatvédelmi Testület (European Data Protection Board, EDPD), https://edpb.europa.eu/edpb_hu

[419] European Data Protection Board, Guidelines 01/2021 on Examples regarding Data Breach Notification, Version 2.0, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en, letöltés: 2022. január 15.

[420] A Ransomware típusú támadás során általában a támadó egy rosszindulatú kód segítségével titkosítja a személyes adatokat, ezt követően a váltságdíjat kér az adatkezelőtől a visszafejtő kódért cserébe.

hozzáférésére vonatkozóan egyaránt, továbbá a megfelelő, hatékony és integrált vírusírtó és kártékony program felderítő és hatástalanító szoftver beszerzése és alkalmazása, a megfelelő, hatékony és integrált tűzfal és behatolásjelző, valamint a forgalomirányító rendszer beszerzése és alkalmazása, a munkavállalók rendszeres információbiztonsági oktatása (támadások felismerése, megelőzése, nem hiteles vagy nem megbízható e-mailek kiszűrése, incidenskezelés – értesítési lánc alkalmazása), a naplókezelési eljárások alkalmazása, a hitelesítési, kulcs- és jelszókezelési eljárás alkalmazása, CSIRT és CERT létrehozása és működtetése szervezeten belül és nemzeti, nemzetközi szinten egyaránt, valamint a kockázatkezelési eljárások alkalmazása annak érdekében, hogy az adatkezelés és az adatfeldolgozás során a GDPR előírásai teljesüljenek. Következő téma az adatszivárgás, külső támadás.[421] Ilyen típusú támadás például az SQL Injection, vagy a webalkalmazások körében ismert sérülékenységi forma az OWASP (Open Web Application Security Project), illetve az LDAP (Lightweight Directory Access Protocol) injektálás. Az SQL Injection egyik leggyakoribb megvalósítása szerint, HTML formok adatbeviteli mezőibe illesztett SQL parancsrészlet felhasználásával gyűjtenek információt, például elsődlegesen felhasználói jelszavak megszerzésének céljából. Ebben az esetben a másodlagos vagy a harmadlagos célpont a támadás valódi célja. Ezáltal a titoktartás és esetleg az adatsértetlenség alapelv sérül. Számos olyan intézkedés áll az adatkezelők (rendszerfejlesztők és rendszerüzemeltetők) rendelkezésére, amellyel jelentősen csökkenthetik a támadás sikeres végrehajtását. A nevezett incidensek elkerülésére, illetve kezelésére vonatkozó EDPD javaslat alapján szükséges olyan hitelesítési módszerek alkalmazása, amelyek elkerülik a jelszavak szerveroldali feldolgozását, továbbá a rendszer naprakészen tartása (biztonsági frissítések), az erős hitelesítési módszerek alkalmazása, különösen kétfaktoros hitelesítések és hitelesítési szerverek használatával, naprakész jelszópolitikával kiegészítve, a biztonságos fejlesztési szabványok, „*brute force attack*” kiszűrése és a tűzfalszabályok, valamint behatolásjelző rendszer hatékony használata, az erős felhasználói jogosultságok kialakítása és hozzáférés-felügyeleti házirend alkalmazása, a rendszeres IT Audit végrehajtása (szimuláció, értékelés, intézkedés), a sebezhetőségek javítása és a támadási kísérletek felderítése, értékelése, a biztonsági másolatok rendszeres tesztelése, a biztonsági rendszerbeállítások alkalmazása (*no session ID in URL*). Következő téma az emberi kockázati tényező (belső). Az elmúlt években az adatvédelmi incidens bejelentési rendszerekkel rendelkező joghatóságok megerősítették, hogy a legtöbb személyes

[421] Az adatszivárgás külső támadás által olyan típusú támadás eredménye, amely során egy adott szolgáltatás sebezhetőségét kihasználva az adatfeldolgozó – általában tudtán kívül – az interneten keresztül harmadik feleknek ad át információkat.

adatot ért adatvédelmi incidenst „*human error*” alapú.[422] A „*human error*” alapú incidensek elkerülésére, illetve kezelésére vonatkozó EDPD javaslat alapján szükséges a képzési, oktatási és tudatosító programok rendszeres alkalmazása, a hatékony adatvédelmi gyakorlatok, eljárások és rendszerek kialakítása, a felhasználói hozzáférési szabályozás betartatása, a hitelesítése eljárások technikai megvalósítása („*force user authentication*”), az adatáramlás ellenőrzése a fájlszerver és a munkaállomások között, az „*I/O interface security*” beállítások („*lock/unlock*”) alkalmazása a BIOS-ban vagy a más vezérlők esetében, a nyílt felhőszolgáltatások tiltása, a nyílt levelezőszolgáltatásokhoz való hozzáférés tiltása és megakadályozása, a képernyőnyomtatás funkció letiltása, a „*tiszta asztal*”, „*tiszta képernyő*” politika érvényesítése, a személyes adatkezelést menedzselő, dedikált rendszerek és informatikai eszközök használata a nem megfelelő kommunikáció és az emberi tévedések elkerülésére. Az adatlopás vagy adatvesztés téma tekintetében gyakori eset a hordozható eszközök elvesztése vagy ellopása. Ezekben az esetekben az adatkezelőnek figyelembe kell vennie az adatkezelési művelet körülményeit, így az eszközön tárolt adatok típusát, a támogató eszközöket, valamint a jogsértést megelőzően megtett intézkedéseket a megfelelő szintű adatkezelés biztosítása érdekében. Az EDPD, az adatlopások vagy –vesztések elkerülésére, illetve kezelésére vonatkozó javaslata alapján szükséges a titkosítási módszerek alkalmazása minden eszközön (Bitlocker, Veracrypt, DM-Crypt), a felhasználói név/jelszó használata minden eszközön, a többfaktoros azonosítás alkalmazása, az eszközmeghatározási funkciók használata, az MDM (Mobile Devices Management) alkalmazás és lokalizáció használata, a központi háttérszerver használata adatmentésre, az automatikus biztonsági adatmentési eljárások használata, a biztonságos VPN használata, lehetőleg kétfaktoros hitelesítési kulccsal, a fizikai védelem szempontjából elengedhetetlen fizikai zár biztosítása az alkalmazottak részére és a mobileszközök védelmére, a vállalati eszközhasználat szabályozása a vállalaton belül, valamint a vállalaton kívül egyaránt, a központosított eszközkezelés (monitoring) alkalmazása, valamint a magán eszközhasználat vállalaton belüli szabályozása, a fizikai hozzáférés-ellenőrzők használata, az érzékeny információk kezelésének szigorítása (merevlemezen vagy hordozható IT eszközökön). Az e-mail vonatkozású incidensek, „félrepostázás” (MISPOSTAL) esetek tekintetében a „*humán faktor*” egyik jelentős kategóriája az emberi figyelmetlenség, amely sok esetben elősegíti az email általi incidensek (adattovábbítás

[422] International Conference of Data Protection and Privacy Commissioners, RESOLUTION TO ADDRESS THE ROLE OF HUMAN ERROR IN PERSONAL DATA BREACHES, 41. International Conference of Data Protection and Privacy Commissioners, Tirana, Albania, sponsor: Office of the Australian Information Commissioner, Australia, 2019.

illetéktelen személynek, email címzettek vagy címlista felcserélése) bekövetkezését. Az adatkezelő megelőzési módszerekkel csökkenteni tudja a figyelmetlenségből eredő incidensek számát. Az EDPD, a „*humán faktor*”, figyelmetlenség alapú incidensek elkerülésére, illetve kezelésére vonatkozó javaslata alapján szükséges a kommunikációs (levél, email küldés) szabályok felállítása és alkalmazása, az alkalmazottak képzése, a „*bcc*” mező használata több címzett esetén, a „*négyszem elv*” használata, az automatikus címzés és címlista használata, az indokoltságtól függő üzenetkésleltetés alkalmazása, a kommunikációs képzések és tudatosítási programok szervezése adatvédelmi tisztviselő támogatásával. Következő téma az egyéb, illetve „*Social Engineering*” módszerek. Az EDPD a hivatkozott esetek által felhívja a figyelmet az előzetes intézkedések jelentőségére. A „*Social Engineering*” módszerek alkalmazása során bekövetkezett jogsértések magas kockázatot jelentenek, mivel sok esetben az érintett magánéletéről (szokások, kapcsolatok) adhatnak információt, és veszélyeztetéshez, anyagi kárhoz vezethetnek (üldözés, testi épség veszélyeztetése). A támadás során megszerzett személyes adatok arra is felhasználhatók, hogy elősegítsék a vállalati email fiók feletti felügyelet átvételét, és további hitelesítési adatokat (banki) is beszerezhessenek. Figyelembe véve a kockázatokat, és magas biztonsági szintű, megfelelő hitelesítési intézkedéseket kell megvalósítani, attól függően, hogy milyen típusú személyes adatokhoz lehet hozzáférni a támadás során. Sok esetben az incidens sokáig észrevétlen marad, ezért az EDPD javasolja az automatizált folyamatok, vezérlések, incidens monitoring és riasztórendszer, válaszintézkedések felülvizsgálatát.

5.6.3.3. A NAIH ÖT LÉPÉSBŐL ÁLLÓ FORGATÓKÖNYVE ADATKEZELŐKNEK

A NAIH szervezete is törekszik az adatkezelők és adatfeldolgozók munkájához útmutatásokat biztosítani. Tekintettel arra, hogy az Infotv. vonatkozásában különféle ellenőrzéseket, mint például az érdekmérlegelési tesztet is kell elvégezni, a munkáltatónak számos szempontot figyelemmel kell kísérnie, ezért a NAIH munkahelyi adatkezelésekről szóló tájékoztatóban öt lépésből álló forgatókönyvet[423] javasol, amelyek az alábbiak:

1. lépés: az adatkezelőnek a tervezett adatkezelés megkezdése előtt át kell tekintetnie, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-

[423] A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről, NAIH, 2016., https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf, letöltés: 2021. december 23.

e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.

2. lépés: az adatkezelői jogos érdek lehető legpontosabb meghatározása.

3. lépés: annak meghatározása, hogy mi az adatkezelés célja, milyen személyes adatok meddig tartó adatkezelését igényli a jogos érdek.

4. lépés: annak meghatározása, hogy az érintettnek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket az érintettek felhozhatnának az adatkezeléssel szemben).

5. lépés: annak meghatározása, hogy miért korlátozza arányosan az adatkezelői jogos érintetti jogokat, várakozásokat. Az érdekmérlegelésen alapuló adatkezelések esetében többek között a fokozatosság elvének érvényesülése és az érintett jelenléte többlet biztosítékként szolgálják az adatkezelés szükségesség-arányosságát.

Az adatvédelmi tájékoztatók és útmutatók számos megoldást nyújtanak az adatkezelők számára, amelyeket követve teljesíthetőek az Infotv. vonatkozó rendelkezései.

5.6.3.4. A NAIH GYAKORLATI ÚTMUTATÓJA ADATKEZELŐK RÉSZÉRE, VÉDETT ADATOT NEM TARTALMAZÓ KIVONAT ELKÉSZÍTÉSÉHEZ

A Hatóság 2014. évben készített anonim adatok előállítását támogató útmutatója segíti az adatkezelőket és az adatfeldolgozókat a személyes adatok kivonatában való elkészítésében, az alábbi instrukciók alkalmazásával:

1. Az anonim adatokat tartalmazó kivonat előállítását lehetőleg olyan, szakmailag kompetens, felelősségteljes döntéshozatalra képes adatkezelő személy koordinálja, vagy teljesítse, aki az átalakítási mechanizmust, a vonatkozó jogszabályokat és a kivonat alapjául szolgáló irat tartalmát is jól ismeri.

2. A folyamat során csak azon adatok távolíthatók el, amelyeket törvény alapján védeni szükséges.

3. A kivonat készítése során a szöveg belső összefüggései nem torzulhatnak, az eredeti szöveg értelmét kell közvetíteni.

4. A törölt adatok helyét egyértelműen meg kell jelölni.

5. Törekedni kell arra, hogy a kivonat az eredeti szöveg arányait megőrizze.

6. Elektronikus közzététel előtt informatikus szakértői vizsgálat szükséges.

7. A papír vagy elektronikus alapú kivonaton a védett adatokat semmilyen módon nem szabad hozzáférhetővé tenni.[424]

5.6.3.5. AZ OTTHONI MUNKAVÉGZÉS OPTIMALIZÁLÁSA MAGASABB SZINTŰ INFORMÁCIÓBIZTONSÁGI INTÉZKEDÉSEKKEL ÉS JOGSZABÁLYI TÁMOGATÁSSAL

A rendszerüzemeltetők, – beleértve az alkalmazásgazdákat is – az információs rendszer rendszergazdái, de egy-egy alkalmazás használatának tekintetében egyben végfelhasználók is, éppen ezért alkalmazniuk kell mindkét funkcióra vonatkozó előírásokat, úgymint az IT és a jogszabályi ajánlásokat és rendelkezéseket egyaránt. A rendelkezések és az IT ismeretek megfeleltetésével és együttes alkalmazásával egy olyan módszer állítható össze, amellyel a biztonságtudatos magatartás fejleszthető, magasabb szintre emelhető, mindez a munkáltató által biztosított vagy akár az otthoni környezetben egyaránt. [425] Saját kutatásom szerint a rendszerüzemeltetői biztonságtudatos viselkedésének szabályait, távoli illetve otthoni munkavégzés esetén a következő pontokba lehet csoportosítani: optimális erőforráskezelés, információvédelem, kommunikációvédelem, incidenskezelés, mentés.

Optimális erőforráskezelés. Az IT erőforrások rendszerfüggő beállítása és használata minden, információs rendszert használóra vonatkozik. Csakúgy, mint a szervezet irodájából, úgy az otthoni környezetből is elláthatják feladataikat a munkavállalók. Optimális erőforráskezelésen érthetünk eszköz és humán erőforrást is, így az információbiztonsági irányelvek mindkettőre vonatkoznak.[426] A távoli munkavégzés feltételeit az Európai Unió már a 2002. évi keretmegállapodással támogatta.[427] A keretmegállapodás az első olyan autonóm megállapodás, amelyet az európai partnerek megtárgyaltak, és mérföldkőnek számít az EU ipari kapcsolataiban. Az európai szociális partnerek és tagszervezeteik nemzeti szinten első alkalommal alapelvek és szabályok meghatározása révén vállalták ezt az új munkaszervezési formát, és vállalták, hogy időben végrehajtják a tagállamokban. A távmunka lényege az internetalapú munkavégzés, amely során a munkavállalók infokommunikációs eszközök

[424] NAIH-1938-2/2013/T, Gyakorlati útmutató védett adatot nem tartalmazó kivonat készítéséhez, NAIH, 2014., https://naih.hu/files/2014_02_03_anonimizalas_gyak_utm.pdf, letöltés: 2022. január 14.
[425] Győrffyné, Holló Krisztina, Információbiztonság, avagy incidens kontra biztonságtudatos viselkedés, INFOKOMMUNIKÁCIÓ ÉS JOG 18., 76 pp. 17-23. 7 p., 2021.
[426] MSZ ISO/IEC 27001:2014 szabvány, Erőforrások kezelése
[427] Európai Munkahelyi Biztonság és Egészségvédelmi Ügynökség, Framework Agreement on Telework https://osha.europa.eu/hu/legislation/guidelines/oshinfo_2001, letöltés: 2020. november 18.

felhasználásával kommunikálnak a kollégákkal és munkáltatóval. A munkavégzés eredményét elektronikusan továbbítják, vagy a feladatokat a kiszolgáló segítségével ún. vastag vagy vékony kliens felületén végzik el. A felmérések alapján megállapították, hogy a „home office" lehetősége a munkahelyen csökkenti a szabadságként kivett vagy betegállományban töltött napok számát, ezáltal növelheti a munkavállalók lojalitását a munkáltató irányába. A távmunkavégzés elterjedése különböző az európai tagállamokban. Az alábbi felmérési statisztika megmutatja, hogy a rendszeresen távmunkát végzők számát tekintve első helyen Hollandia, Finnország, Luxemburg és Ausztria áll (10-14%), míg Magyarország 2018-ban 2,3 és 2019-ben 1,2 %-kal tölti be helyét a rangsorban. (A távmunkavégzés aránya az Európai Unióban, 2018.[428], A távmunkavégzés aránya az Európai Unióban (nyugati országok), 2016-2019., A távmunkavégzés aránya az Európai Unióban (Magyarország), 2016-2019. [429]) A távoli munkavégzésnek nemcsak humán erőforrás szabályozási vonzata van. A „*home office*" megkezdése előtt, az eszközök erőforráskezelése során be kell állítani az IT rendszert, így kiszolgáló oldalról különösen a routerek, szerverek (fizikai és virtuális), operációs rendszerek, adatbáziskezelő rendszerek és alkalmazások, valamint a kommunikáció, a hozzáférés konfigurálására és működésére vonatkozóan. Továbbá ellenőrizni kell a végfelhasználói és a kiszolgálói erőforrásokat, és a rendelkezésre álló kapacitást is. Az információs rendszerek fejlesztésekor meghatározott és az alkalmazásukhoz kötött, illetve a felhasználásukkal elvégzendő feladatellátáshoz igazított kiszolgálói és végfelhasználói minimális hardver, szoftver követelményt a távoli munkavégzés kialakítása során is teljesíteni kell. A minimális követelmények rendelkezésre állása nélkül a rendszergazdai vagy felhasználói feladatteljesítés rovására mehet, úgymint minőségromlás, vagy csökkenő rendelkezésre állás. A munkáltató a minimális IT követelmények ismeretében a távoli munkavégzést a követelmények teljesítéséhez igazíthatja, tehát a távoli munkavégzés előfeltételeként szabhatja meg. A szükséges végfelhasználói vagy üzemeltetői erőforrások rendszerenként változó, éppen ezért kizárólag csak rendszerspecifikus szabály rögzíthető. Az ISO/IEC 27001 Információbiztonsági Irányítási Rendszer követelménye alapján a szervezetnek meg kell határoznia és biztosítania kell az információs rendszer kialakításához, bevezetéséhez, fenntartásához és folyamatos

[428] Országgyűlés Hivatala, Infojegyzet 2020/7 https://www.parlament.hu/documents/10181/4464848/Infojegyzet_2020_7_tavmunka.pdf/80c2a726-b98d-0c81-363e-1f1023acab8e?t=1585506935186, letöltés: 2020. november 18.

[429] Eurostat, Employed persons working from home as a percentage of the total employment, by sex, age and professional status (%) https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=lfsa_ehomp&lang=en, letöltés: 2020. november 18.

fejlesztéséhez szükséges erőforrásokat.[430] Az erőforrások használatát folyamatos megfigyelés (erőforrás monitoring) alatt kell tartani, optimalizálni kell és meg kell határozni a szükséges kapacitást (informatikai fejlesztési terv), ezáltal biztosítani lehet az üzletmenet-folytonossági szabályok teljesítését is. Az egyre bonyolultabb elvárások és megoldások összetettebb információbiztonsági konfigurációs beállításokat kezelő IT eszközök alkalmazását követeli meg, így van ez a szerverek, hálózati eszközök alkalmazásának esetében is.

Információvédelem. Csak a feltétlenül szükséges eszközöket és információkat „*vigye haza*" elv gyakorlati alkalmazása jelentős és biztosítani kell a távoli munkavégzés információbiztonsági feltételeit. A technikai megvalósítás szintjén a biztonságos VPN kapcsolat lehetőséget nyújt a távoli munkavégzésre, így a szerverek távoli üzemeltetésére is. A hivatali információs hálózat, tárhely és szerver használatával minimálisra csökkenthető az adattovábbítás a saját eszközre. A munkáltató tulajdonában lévő eszközök, úgymint PC, laptop vagy egyéb tárhely használatának előírásával a munkavégzés során a munkáltató kötelezheti a munkavállalót ezen eszközök kizárólagos használatára. Az egyes feladatmegoldáshoz, az elvárt, megfelelő minőségű kommunikációhoz elengedhetetlenül szükséges a minimális informatikai konfigurációs-követelmények teljesítése, mind a szerver, mind pedig a végfelhasználói oldalról. A különböző funkciót betöltő kiszolgáló szerver(ek) esetében ez tevékenység nagymértékben szerteágazó, így különösen a root-config, DNS, valamint hozzáférés szabályozást,a tűzfal konfigurálását (forgalomirányítás, forrás Routing, hozzáférés és IP Spoofing kezelés, csomagszűrés, integrált proxy vagy alkalmazás átjáró konfigurálás, behatolásfelismerés, címfordítás, portkezelés és –szűrés, intranet, backup az esetleges helyreállítás céljából stb.), a VPN konfigurációt (engedélyezett portok és tesztelése), az alkalmazás konfigurációit (webes vagy vastag kliens esetében egyaránt), a tárhelykapacitást (szerver szinten és szerveren belül egyarán, mivel egyes adatbáziskezelő rendszerek külön-külön követelik meg a táblatér beállításokat), az engedélyezhető maximális felhasználói hozzáférések számát, köztes szerver esetében a szerverek közti kommunikációt vagy a hozzáférést, vagy az eseménykezelés feladatait érinti. A szerverbeállítások a célzott feladat szerint eltérőek lehetnek, a fenti felsorolás csoportosítva adja meg a szükséges rendszergazdai feladatokat. Természetesen mindegyik feladattípus többnyire egy-egy szerver (általában virtuális) vagy forgalomirányító szerepét tölti be. VPN üzembe helyezésekor felhasználói teszteket kell végezni annak érdekében, hogy a védett kommunikáció megfelelően van-e konfigurálva, tehát a felhasználó eléri-e a szükséges szervereket, a kliens-szerver közti kapcsolat mennyire gyors és biztonságos. A rendszergazdák

[430] MSZ ISO/IEC 27001:2014 szabvány, Erőforrások kezelése, Az Üzemeltetés biztonsága

az információbiztonsági alapelveknek megfelelő módon beállított IT rendszerrel sok időt és bosszúságot takaríthatnak meg és a továbbiakban a szerverpark felügyeletére és fejlesztésére összpontosíthatnak. Az információvédelmet az Európai Tanács is szigorúan kezeli, ez mutatja az általa kiadott határozat, amely szerint a kommunikációs és információs rendszerek tekintetében az információvédelem azt jelenti, hogy képes megvédeni az általuk kezelt adatokat, valamint a szükséges módon, a szükséges időben, a jogszerű felhasználók ellenőrzése alatt működnek. A hatékony információvédelem biztosítja az adatok megfelelő minősítési szintjét, sértetlenségét, rendelkezésre állását, letagadhatatlanságát és hitelességét. Az információbiztonsági szabályok alkalmazásának, valamint a benne foglalt információkategóriaalkotás jelentőségét, továbbá az adatok osztályozásának szükségességét tükrözi az Európai Unió Tanácsa által, a minősített adatok védelmét szolgáló biztonsági szabályok meghatározására vonatkozó határozata is, amely szerint a minősített adatokat négy minősítési szintbe sorolja, figyelembe véve sérülésük, elvesztésük, vagy eltulajdonításuk milyen következményekkel járna.[431] A „*confidentiel ue/eu confidential"* vagy magasabb szintű minősített adatok esetében abból a célból is biztonsági intézkedéseket kell alkalmazni, hogy a nem szándékos technikai behatás miatt a minősített adatok bizalmas jellege ne sérüljön. Ezen biztonsági intézkedések az úgynevezett „*tempest"* biztonsági intézkedések.[432] A kategóriák megalkotása mintául szolgálhat a hazai és nemzetközi intézmények által kezelt, nemcsak minősített adatok, hanem személyes vagy akár üzleti információ biztonsági osztályba sorolásához. A személyes adatok kategóriáinak meghatározását az Infotv. is rögzíti. Jelen tanulmányban a minősített adatok kategorizálásának módszerét az intézmények számára követendő példaként kívántam megemlíteni, mivel tapasztalatom szerint adatvédelmi szabályzat kialakításakor, az adatkategóriák meghatározásánál jelentős nehézségekkel találkozhatunk. Adott esetben előfordulhat információbiztonsági és adatvédelmi szabályok, vagy akár tévesen használt, adatbázisstruktúra szerinti fogalommeghatározás is. Tekintettel arra, hogy az alábbiakban leginkább az információbiztonsági irányelvekre összpontosítok, a

[431] „très secret ue/eu top secret": az információk engedély nélküli hozzáférése rendkívül súlyosan sértheti az Európai Unió, illetve a tagállamok alapvető érdekeit,
„secret ue/eu secret": az információk engedély nélküli hozzáférése súlyosan sértheti az Európai Unió, illetve a tagállamok alapvető érdekeit,
„confidentiel ue/eu confidential": az információk engedély nélküli hozzáférése sértheti az Európai Unió vagy a tagállamok alapvető érdekeit,
„restreint ue/eu restricted": az információk engedély nélküli hozzáférése hátrányosan érintheti az Európai Unió vagy a tagállamok érdekeit.

[432] Európai Unió: A Tanács Határozata (2013. szeptember 23.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2013/488/EU), Brüsszel, 2013. https://eur-lex.europa.eu/legal-content/hu/TXT/PDF/?uri=CELEX:32013D0488&from=EN letöltés: 2020. november 17.

tartalmi és a mennyiségi korlátok miatt csak az adattípusok megemlítését, osztályozásának szükségességét és pontosságának jelentőségét és az irányelvekkel való kapcsolatát emeltem ki. A személyes adatvédelemre vonatkozó Uniós rendelet[433] célja a személyes szabadság és az alapvető jog védelmének biztosítása, az uniós intézmények és szervek által végzett személyes adatkezeléssel kapcsolatban. A rendelet azokat az elveket és kötelezettségeket határozza meg, melyeket az uniós intézményeknek a személyes adatok kezelése során be kell tartaniuk.

Az információvédelmi szabályok alkalmazásakor figyelembe kell venni a szervezet IT hozzáférésre vonatkozó előírásait, különös tekintettel a követelményekre és a jogosultságkezelésre.[434] A hozzáférési szabályokat és a jogosultságkezelési eljárást a szervezet tulajdonában vagy birtokában lévő információk adatkezelése, adatfeldolgozása vagy adattovábbítása, illetve azokhoz tartozó műveletek (adatrögzítés, lekérdezés, módosítás, törlés, biztonsági mentés), adatkategóriába sorolása, továbbá tárolási helye, illetve az információs rendszer típusa (DB, mail, OS stb.) és a rendelkezésre álló IT alapján lehet meghatározni. A jogszabályi információvédelemnek megfelelve az információs rendszerekben fizikai és logikai védelmet kell megvalósítani, aminek elsődleges felelősei az informatikai rendszerek üzemeltetői.

Kommunikációvédelem. Az információs rendszer biztonsági besorolásának megfelelően kell védeni az otthoni hálózatot is és a biztonságos kapcsolatok segítségével szabad kommunikálni a külvilággal. Az információbiztonsági alapelveknek megfelelően a kommunikációbiztonság szabályaihoz tartozik a hálózatbiztonság és az információátvitel,[435] amely szerint biztosítani kell a hálózatokban lévő információk és azokat támogató információfeldolgozó eszközök védelmét, valamint fenn kell tartani a szervezeten belüli és a partnerek általi információátvitel biztonságát. A szabvány szerint a hálózatokat működtetni és felügyelni, ezért a hálózati szolgáltatásokra meg kell határozni a biztonsági mechanizmusokat, a szolgáltatási szinteket és a kezelési követelményeket. A különböző biztonsági besorolású információtípusok és szolgáltatások csoportjait elkülönítve kell kezelni. Minden típusú elektronikus üzenetküldést megfelelő logikai és fizikai védelemmel kell ellátni annak érdekében, hogy a csomag a feladótól a címzett eszközhöz vagy személyhez biztonságban megérkezzen. Az információtípustól

[433] Európai Unió: Az Európai Parlament és a Tanács (EU) 2018/1725 Rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32018R1725&from=EN letöltés: 2020. november 17.
[434] MSZ ISO/IEC 27001:2014 szabvány, Hozzáférés-felügyelet
[435] MSZ ISO/IEC 27001:2014 szabvány, A hálózat biztonsága, Információátvitel

függően tárolás során az elektronikus információkat, adatokat megfelelő védelemmel kell ellátni, a hozzáféréseket szabályozni kell és amennyiben a jellege szerint szükséges, az adatkezelők, adatfeldolgozó, adattovábbítók kizárólag titoktartási megállapodással teljesíthetik feladataikat. A kommunikációvédelem a közvetlen és a közvetett módon megvalósult információcserére, -átvitelre egyaránt vonatkozik. Jelent esetben csak az információelméletre[436] épített, közvetett, digitális alapú kommunikációval foglalkozunk. Az információelmélet szerinti csatornába kapcsolt intelligens eszközök közötti biztonságos információátvitelt megfelelő technológiával kell biztosítani. Az ISO/IEC 27000-es szabványcsalád az információ biztonságos kezelését, továbbítását, vagy akár a jelátvitel logikai és technikai elveit és ajánlásait rögzíti, ezen túlmenően az elveket felhasználva az Uniós ajánlások és előírások keretén belül megfogalmazták az adatvédelemre (GDPR), minősített adatok kezelésére és védelmére[437], vagy akár az ajánlott technológiák alkalmazására vonatkozó előírásokat, ajánlásokat[438]. Az Európai Unió Tanácsa is javasolhat IT eszközt, mint például a CryptoGuard VPN átjárót, ami gyors és biztonságos (AES 256) hang-, video- és adatátvitelt biztosít kis és nagy hálózatokban, megfelelő a virtuális magánhálózatok titkosításához és biztonságához. Tekintettel az informatikai technológiák dinamikus fejlődésére, a Tanács által közzétett IT eszközpaletta minimális követelmény és ajánlás lehet. Itt a hangsúly az alkalmazandó eszköz biztonsági konfigurációs beállíthatóságán van, amely nem lehet alacsonyabb biztonsági szintű, mint a Tanács által meghatározott. Amennyiben mégis szükség van a magánhálózat és az otthoni tárhely használatára, úgy a kommunikációra vonatkozó információbiztonsági előírások betartása elengedhetetlen, különösen a kommunikáció biztonságára, úgymint a VPN, az e-mail és levelezőrendszer, vagy az okostelefon használatára, a hozzáférésre, úgymint jelszó policy, fiókvédelem, szoftveres védelem, hitelesítés, tartalomszűrés, az adatkezelésre és az adattárolásra (titkosítás), adattovábbításra (titoktartás, továbbítás harmadik fél részére), az adatbiztonságra és –védelemre, például tanúsítvánnyal rendelkező vírusírtó, kémprogramfigyelő használatára vonatkozó rendelkezések és ajánlások gyakorlati megvalósítása tekintetében. A szükséges információbiztonsági beállításokat, mint

[436] Claude Elwood Shannon: A Mathematical Theory of Communication (The Bell System Technical Journal), és Norbert Wiener: Cybernetics or Control and Communication in the Animal and the Machine című műve, 1948.
[437] Európai Unió: A Tanács Határozata (2013. szeptember 23.)az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2013/488/EU), Brüsszel, 2013. https://eur-lex.europa.eu/legal-content/hu/TXT/PDF/?uri=CELEX:32013D0488&from=EN letöltés: 2020. november 17.
[438] Az Európai Unió Tanácsa: Approved cryptographic products – secret ue/eu secret, List of Approved Cryptographic Products (LACP)

például a hitelesítés vagy a tartalomszűrés szabályait funkciótól függően az adott alkalmazás-, DB vagy mailszerver esetében is alkalmazni kell.

Incidenskezelés. Kiemelt figyelmet kell fordítani az incidenskezelésre. Amennyiben bármely otthoni informatikai eszközén rendellenes viselkedést tapasztalható, haladéktalanul meg kell kezdeni az elhárítást, offline állapotban (logelemzés, vírusírtás, helyreállítás). Ha támadási kísérlet gyanúja merül fel a hivatali eszközökön vagy az üzemeltetett, hálózatba kapcsolt IT eszközökön, mielőbb meg kell kezdeni a felderítést és a hibaelhárítást az incidenskezelésre vonatkozó előírásoknak megfelelően. Az incidenskezelés jelentőségét az is mutatja, hogy nemcsak szabványi szinten, hanem Uniós szinten is foglalkoznak a szabályozással és a gyakorlati megvalósítással. Szabványi szintű ajánlás például az eseménykezelés, a monitoring, a gyengeségek feltérképezése és kezelése, események feldolgozása, megelőzése és védelmi intézkedések tudatosítása.[439]

Mentés. Az adatokat biztonságos területre kell menteni, szükség esetén a redundáns adatmentést kell alkalmazni. A szerver oldali adatmentéskor teljesíteni kell az adatmentés szabályaira vonatkozó követelményeket, különösen az Infotv. jogszabály által előírt rendelkezéseket, különösen a tárolás, adatkezelés, adattovábbítás tevékenységekre vonatkozóan. Az adatmentési tevékenység a szervezet információbiztonsági politikájához és szabályozásához kell igazítani, különösen az információvédelmi előírásokhoz. Mentés céljából másolatokat kell készíteni az információkról, szoftverekről és rendszerképekről, szükség esetén eseménynaplókról és rendszeresen tesztelni kell a mentési szabályt az előírásoknak és a konfigurációs beállításoknak megfelelően. A mentési teszteket ellenőrizni kell. A szervezetnek információbiztonsági szempontból teljesítenie kell a redundáns adattárolás megvalósítását, lehetőleg különböző földrajzi helyen.[440] A következő instrukciók a rendszerüzemeltetőkre ugyanúgy vonatkoznak, mint a végfelhasználókra, ezért ezen pontok részletesebb kidolgozása ebben a tanulmányban kevésbé releváns. Up-to-date" – legyen naprakész minden alkalmazás, minden eszközön. Mikrofon és webkamera biztonságos kezelése: csak indokolt esetben legyen bekacsolva. Személyes és üzleti információkat, tevékenységet el kell különíteni egymástól. Szervezőként az online találkozók összes résztvevőjét azonosítani kell, részvevőként pedig legalább a szervezőt. „Tiszta asztal, tiszta képernyő" elv alkalmazása „home office"-ban is javasolt. Gyanús e-maileket, mellékleteket, hivatkozásokat, képeket egyáltalán nem, vagy csak kellő óvatossággal szabad megnyitni. Az online szakmai megbeszélések és tréningek fejlesztik

[439] MSZ ISO/IEC 27001:2014 szabvány, Az információbiztonsági incidensek kezelése
[440] MSZ ISO/IEC 27001:2014 szabvány, Az üzemeltetés biztonsága, Mentés

a szakmai tudást, az együttműködést és magasabb szintre emelik az információbiztonság tudatos viselkedést.

A felhasználói megfontolt aktivitásra nem lehet minden esetben számítani. A Nemzetközi Távközlési Unió által kiadott információk szerint 2016. évvégén a világ népességének 47 százaléka használta az internetet. Egy nagyobb cégnél több tízezer ember rendelkezik informatikai rendszer hozzáféréssel. A számos, különböző jogosultság szintű hozzáférést tekintve elég egy figyelmetlen vagy képzetlen felhasználó és a legfontosabbnak tartott védelem máris veszélybe került. A hazai biztonságtudatosság helyzetét vizsgálva is hasonló megállapítás született, ami szerint az üzleti és a közszférában dolgozók több mint harmada úgy gondolja, hogy a számítógépük nem potenciális célpontja egy rosszindulatú támadásnak.[441] A nagyszámú kiberbűnözés is indokolttá teszi a felhasználók folyamatos tanulását és a tájékozottság fontosságát. Lépést kell tartani nemcsak a technikával, az új eszközökkel és alkalmazásokkal, de a veszélyekkel és a megelőzési lehetőségekkel is. A kiberbűnözés hírnévromboló és gazdasági károkozó, így fontos, hogy minden felhasználó tisztában legyen az őt fenyegető támadással. [442]

5.7. RÉSZÖSSZEFOGLALÁS

A „*humán faktor"* információbiztonsági tudatosság hiányosságait kihasználó, „*Social Engineering*" [443] jellegű támadási módszereket és technikákat 2008 óta vizsgálom. Az alábbiakban azokat a tényezőket foglalom össze, amelyek az információbiztonság tudatosításával kapcsolatos kutatásom során állapítottam meg. A kutatásom tevékenységét nagy mértékben segítette az ISO 27001 és 9001 nemzetközi (IRCA által tanúsított) vezető auditori szakképesítésem, továbbá a Nemzeti Közszolgálati Egyetem, Vezető- és Továbbképzési Intézete által szervezett közszolgálati továbbképzés keretében elvégzett oktatói, valamint e-szeminárium vezetői és gyakorlatvezetői tanúsítvány adta szakértelem. A következtetések a harmadik (H3) és a negyedik (H4) hipotézisem vizsgálatához és bizonyíthatóságát, illetve a

[441] Kiss Attila, Krasznay Csaba, A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai, Információs Társadalom, XVII. évf. (2017) 1. szám

[442] Sok veszélyt tartogat a jövő év a vállalkozások számára, http://www.biztositasiszemle.hu/cikk/elemzesek/NULL/sok_veszelyt_tartogat_a_jovo_ev_a_vallalkozasok_szamara.6201.html, letöltés: 2021. december 10.

[443] Kevin D. Mitnick, William L. Simon, The art of deception, „*A social engineering a befolyásolás és a rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social emgineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.*" 2003

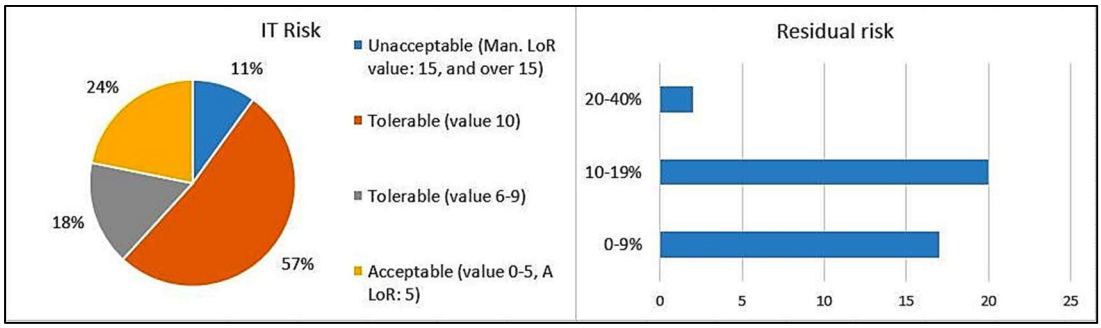
feltételezések elvetését szolgálják. Munkahelyemen végzett tevékenységem és kutatásaim során megállapítottam, hogy az alacsony szintű információbiztonság oka nemcsak informatikai, technológiai jellegű[444] lehet, hanem emberi és szervezési probléma is, mivel a támadások egyik tényezője a „*humán faktor"*. Az ember az, aki az informatikai rendszereket és eszközöket tervezi, megalkotja, konfigurálja és munkavégzés vagy szórakozás céljából felhasználja, hozzáfér személyes és ipari, kutatási adatokhoz. Az ember lehet elkövető, de megtévesztett személy is, aki felhasználható a célszervezet vagy célrendszer adatainak eléréséhez. Az elkövetők a legtöbb esetben célzottan támadnak munkavállalókat és intézményeket, valamint magánembereket egyaránt, károkozási és haszonszerzési célból, egyre modernebb technikával. A „*Social Engineering*" jellegű támadásokat nehéz beazonosítani, sok esetben csak később mérhető fel a kár mértéke. A kibertér adta lehetőségeket tudatosítani csak akkor tudjuk, ha ismert a sérülékenység és a fenyegetés és ezeket mintegy kihívásként és kezelendő tevékenységként ültetjük be a napi feladatok közé. Ha megnevezzük és tudatosítjuk a támadási lehetőségeket és sebezhetőségeket, és a megoldási folyamat az elhárítási módszerek palettájával egyfajta koreográfiaként kerül publikálásra, úgy az intézkedés is napi rutinná válhat. Egy jó hatékonysággal összeállított akcióterv megfelelően leegyszerűsített változata, amely könnyen elsajátítható és kis lépések sorozata, megkönnyíti elfogadhatóságát és alkalmazhatóságát. Véleményem szerint a hangsúly nem a gyógyításon, hanem a megelőzésen van. Az állampolgárokat rendszeresen tájékoztatni kell[445] nemcsak az informatikai lehetőségekről, de az esetleges veszélyekről és a mulasztásból eredő veszteségekről, amelyek mértéke csökkenthető a megfelelő szintű tudatosítással és felkészültséggel. A felhasználói szférának olyan biztonságtudattal kell rendelkeznie, hogy ne fogjon ki rajta az átverés művészete és nagyobb hangsúlyt kell helyezni a szisztematikus képzésre és a tudatosításra. A digitális kompetencia információbiztonsági készsége gyermekkortól az időskorig kialakítható, de

[444] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), letöltés: 2019. november 23.
„*A kiberbiztonság nemcsak technológiai kérdés, hanem olyan, ahol az emberi magatartás is legalább olyan fontos. Éppen ezért határozottan ösztönözni kell a „kiberhigiéniát", azaz olyan egyszerű rutinintézkedéseket, amelyek rendszeres végrehajtásával és elvégzésével a polgárok, a szervezetek és a vállalkozások minimálisra csökkenthetik a kiberfenyegetések kockázatainak való kitettségüket.*"

[445] Nyikes Zoltán, A biztonságtudatosság fejlesztésének egyes lehetőségei, Óbudai Egyetem, A XXII. Fiatal műszakiak tudományos ülésszak előadásai, Műszaki tudományos közlemények 7., Erdély, 2017
„*Mindig az embert kell meggyőzni arról, hogy tegyen magáért, az egészségéért még a betegséget megelőzően, így a kiberbiztonság tekintetében is magának az embernek a biztonságtudatosságát kell növelni az elkerülhető incidensek megelőzésének érdekében.*"

rendkívül időigényes folyamat, ahol az igény, az átadandó tudás és az elfogadás, valamint a készség szintű felhasználás együttesen kell, hogy megvalósuljon. Az egységes, intézményi utasítás már nem elegendő. Folyamatosan javítani kell a vállalati és a közszférában dolgozó állampolgárok biztonságtudatossági állapotán, amelyhez a mindennapi munkavégzés folyamataiba be kell építeni a személyes és online, a vállalati csoportos vagy egyénre szabott konzultációkat, továbbképzéseket és tréningeket. A diákok képzésébe minden képzési szinten és minden korosztály számára elérhetővé kell tenni az először még csak a játékos, majd egyre több információbiztonsági tematikát tartalmazó képzéseket, ezzel elősegítve a digitális kompetencia és a „*kiberhigiénia*" megteremtését és fejlesztését. A végrehajtott, információbiztonsági és minőségirányítási auditok, az emberi tényező biztonságtudatosságának felmérésére, és incidensekre irányuló vizsgálatok és statisztikai adatok, valamint az informatikai oktatások során az tapasztalható, hogy annak ellenére, hogy az adott intézmény vagy vállalkozás rendelkezik a felhasználókra vonatkozó IT biztonsági szabályzatokkal, vezetői utasításokkal, eljárásokkal, a hiányzó vagy a nem megfelelő aktivitás hozzájárul a biztonságtudatosság csökkenéséhez. A kutatásom során megállapítottam, hogy a munkavállalók többsége nincs tisztában az őket érintő fenyegetésekkel, azok realitásával, más esetben azokat tudatosan figyelmen kívül hagyják, ezért esetenként szánt szándékkal, tudatosan megkerülik a kialakított kontrollokat, vagy megszegik a biztonsági szabályokat. Tipikusan csak akkor ismerik fel a biztonságtudatos magatartás és a szabályoknak megfelelően történő eljárások fontosságát, amikor már az incidens megtörtént. Az incidensek számossága mögött többféle esettípus megállapítható, így például az úgynevezett alkalmazotti átveréssel – aminek szintén több fajtája is ismert, különösen a kéretlen levél vagy egy vállalati levélnek álcázott online adatbekérés – viszonylag könnyen hozzájuthatnak a hackerek a szükséges üzleti, pénzügyi és személyhez kötött információkhoz, mert mindig van egy gyenge láncszem vagy egy beépített ember, aki az adatszivárgást véletlenül vagy szándékosan segíti. A jelen fejezetben hivatkozott saját és nemzetközi kutatási statisztikai adatok, valamint a digitális kompetenciafejlesztésre irányuló fejlesztésre irányuló törekvések is alátámasztják a digitális kompetencia, biztonságtudatos képesség fejlesztésének jelentőségét és a hiányos biztonságtudatos tevékenység magánszemélyeket és gazdaságot ért károkozásának súlyosságát. Auditori tevékenységem, vezetőségi átvizsgálása során megállapított eredmények és kutatási adataim szerint a biztonságtudatosság folyamatos fejlesztése elengedhetetlenül szükséges, mivel az elmaradt rendszeres munkavállalói IB és IT képzések és tréningek, valamint vezetői megbeszélések következtében egyes területeken (úgymint naplóellenőrzés, szerverszobára

vonatkozó követelmények teljesítése, jogosultságellenőrzés, szigorúbb hálózati konfigurációs beállítások alkalmazása, ellenőrizetlen elektronikus kommunikáció) hiányosságot tapasztaltam, amely IB szempontból sérülékenység és a vonatkozó kockázat megnövekedését jelentette. A harmadik hipotézisem (H3), amely szerint feltételeztem, hogy a Magyarországon érvényes és intézményi adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését és a szervezet információbiztonsági tudatosság szintjét, jelen fejezetben található, a „*humán error*" okozta kár megelőzésére irányuló legfőképp tudatosítási módszerek az adott szervezetnél való alkalmazásának tapasztalataival és kutatásom során eredményül kapott statisztikai adatokkal igazoltam, amelyet megerősítettem a nemzetközi statisztikai adatok hivatkozásával, valamint a hatóságok, különösen az Európai Adatvédelmi Testület adatvédelmi és információbiztonsági tudatosításra vonatkozó iránymutatásával. A kutatásom során megállapítottam, hogy az IT intézkedések adatvédelmi és információbiztonsági alapelvek szerinti, az IB tudatosítást követő megelőzési tevékenységek alkalmazásának következményeként, az adott területenként (ISMS, ISO 27001, A melléklet) összegyűjtött kockázatfelmérésből származó, összesített átlagértéket megvizsgálva (ALARP módszer figyelembe vételével) összességében kezelhető kockázati szintet eredményeznek. A vizsgálat során megállapítottam, hogy a módszer alkalmazásával a megállapított, kezelendő kockázatok 57%-a elfogadható és csak 11%-ban nem elfogadható, tehát kezelendő kockázati érték tartományába esett. Maradványkockázat vizsgálatakor megállapítottam, hogy a kockázatfelmérés kezelendő 39 esetéből összesen 2 rendelkezett magas maradványkockázati értékkel, ami az 550 vizsgált esethez (sérülékenység és lehetséges fenyegetettség) képest elfogadható érték.[446] (22. ábra)



22. ábra, Kockázatkezelés, elfogadható kockázatok eloszlása, maradványkockázat saját információbiztonsági és kockázatkezelési kutatás alapján, időszak: 2015-2020.

[446] Krisztina Győrffyné Holló, Adam Karisztl: Domino effect and other models in the it process, Gradus Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

Az negyedik hipotézisem (H4) szerint feltételeztem, hogy az információbiztonsági tudatosítás rendszerét nemcsak az informatikai oktatásban, hanem minden korosztály számára elérhetővé kell tenni és minden szakterületen indokolt bevezetni és működtetni. A jelen fejezetben ismertetett információbiztonsági tudatosság képzéseire irányuló ENISA 2020. és 2021. évi felmérése, statisztikai adatokkal támasztja alá, hogy az IB oktatást minden korosztály számára biztosítani kell. Az IB oktatásra irányuló Európai Bizottság digitális oktatási cselekvési terve (2020.) az általános- és középiskolákra, valamint a felsőoktatásra egyaránt összpontosít. Az EU statisztikai adataival és a kutatási eredményeim statisztikai adataival igazolható a negyedik (H4) hipotézis. A NAIH 2017. évi felmérése is igazolja, hogy az óvodás gyermekek jelentős része (30%) már rendelkezik saját digitális eszközzel, az általános iskolás, alsó tagozatos gyermekek (60%-nak volt saját digitális eszköze 2017-ben) tekintetében pedig elvárás a digitális oktatásba való becsatlakozás. Ezek az elvárások és számok azt jelentik, hogy első osztályban elkezdeni a gyermekek digitális kompetenciafejlesztését, elvárt feladat, ugyanakkor a NAIH felmérése és a tapasztalat is azt mutatja, hogy a kezdeti, játékos digitális felkészítéseket már óvodás korban el kell kezdeni és bele kell építeni az iskolafelkészítő tevékenységek közé. Véleményem szerint a szülőket szülő értekezletekkel egybekötött IB tájékoztatásban kell részesíteni annak érdekében, hogy otthoni körülmények között is megfelelően felkészíthessék gyermeküket a digitális eszközök információbiztonság-tudatos használatára.

6. ÖSSZEGZŐ MEGÁLLAPÍTÁSOK, KÖVETKEZTETÉSEK ÉS FEJLESZTÉSI JAVASLATOK

Az információbiztonság régóta létező, de korábba nem definiált fogalom, amely az idők folyamán folyamatosan változott, és igazodott a történelmi korokhoz. Megfogalmazása és kutatása lényegtelen volt egészen a technikai forradalomig, az információelmélet megalapozásáig. Az információbiztonság, mint új jogintézmény a szűkebb értelemben vett személyes, üzleti, valamint közigazgatási adatbiztonság megvalósítását jelenti az informatikai hálózatok és rendszerek hazai és nemzetközi szabályozásának tekintetében. Az információbiztonság technikai megvalósítása és országos vagy közigazgatási kiterjedésű szabályozása nem korlátozódhat a számítástechnikára, mivel feltétlenül figyelembe kell venni az anyagi és a szellemi tevékenység világában felmerülő biztonsági és védelmi igényeket is. Az információ, valamint az ahhoz tartozó folyamatok, rendszerek és eszközök jelentős személyes, vagy intézményi eszmei és dologi értéket, adatvagyont képeznek, ezen kívül olyan kiemelt jelentőségű erőforrás, amely semmi mással nem helyettesíthető. A közigazgatás intézményei, továbbá az elektronikus információs rendszerek működtetéséért felelős szervezetek egyre gyakrabban szembesülnek különböző eredetű biztonsági fenyegetéssel, így gazdasági, ipari visszaéléssel, számítógépes csalással, szabotázzsal, vandalizmussal, tűzzel vagy árvízzel, de egyre nagyobb fenyegetést jelent a kibertér bűnözése is. Az intézmények fenntartása és rendeltetés szerinti működtetése csak a szükséges és elégséges információ birtokában valósítható meg. Ha az információ nem férhető hozzá, sérült vagy illetéktelen kezekbe jut, az a közigazgatás területén is jelentős anyagi és erkölcsi károkat okozhat, ezért védeni kell. Az újabb és újabb védelmi és biztonsági intézkedések bevezetése azt mutatja, hogy amit egyszer titkosítás alá vontak, később biztosan megfejtik. Éppen ezért teljes biztonságról, illetve teljes védelemről nem beszélhetünk. A XXI. századot egy, az ipari forradalomhoz mérhető információs forradalom okozta változás jellemezi, ahol jelentős szerepet kap a kockázatismeret és a biztonságtudatos tevékenység. A kibertér és környezete egy új dimenzióba helyezte világunkat. Ahol a kiberbűnözés sikeresen megtelepszik, ott folyamatosan bővül, nem törődve az ország és egyéb fizikai határ korlátaival. A kibertér nehézségei, így a sérülékenységek, biztonsági rések, és az azokat kihasználó incidensek következményei már nemcsak a szervezetek, az állami intézmények, de a háztartások életét, ezáltal gyermekeink életét is

negatívan befolyásolja[447] [448], ezen kívül komoly gazdasági és személyt érintő károkat okoz.[449] Éppen ezért ez az adatvédelmi és információbiztonsági rendelkezések nem hagyhatók figyelmen kívül. A folyamatos támadások miatti megelőzési és védekezési, adatvédelmi és információbiztonsági intézkedések sem biztosítanak teljes körű védelmet, de a kockázatok ismerete és ennek megfelelően kidolgozott akciók végrehajtása csökkentheti az esetleges incidensek számát. Ebben a fejezetben összefoglalom kutatásom következtében képződött hipotézis megállapításokat és tudományos eredményeket.

6.1. ÖSSZEGZŐ MEGÁLLAPÍTÁSOK, KÖVETKEZTETÉSEK

6.1.1. HIPOTÉZISEK IGAZOLÁSA

Kutatásom középpontjában az informatika világához szorosan kapcsolódó információbiztonsági tudatosság vizsgálata szerepel. Az adatkezelő egyik legfontosabb feladata és kötelezettsége az érintettek jogainak védelme, a fenyegetések és a kockázatok csökkentésére irányuló megfelelő technikai és szervezési intézkedések végrehajtása.[450] Az értekezés témája az információbiztonsági tudatosság fejlesztésének szükségességére összpontosít, amelyhez az alábbi hipotéziseket igazoltam.

Az első hipotézisem (H1) szerint feltételeztem, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és jogszabályi rendelkezések az informatikai technológiai változásokkal, továbbá a nemzetközi szabványügyi intézmények ajánlásaival és az európai szabályozással összhangban vannak, és egyben kielégítik a hazai információbiztonsági szabályozási igényeket. A második fejezet bemutatja az információtörténet, az adatvédelem, és az információelmélet tudományos elméleteit és összefüggéseit. Az informatikai tudomány megjelenése óta az informatikai tudomány és az információbiztonság különböző fejlődési

[447] Nemzeti Adatvédelmi és Információszabadság Hatóság, Tájékoztatók, ajánlások, Interneten elkövetett bűncselekményekre hívja fel a figyelmet a linken elérhető videó, https://www.naih.hu/tajekoztatok-ajanlasok, Say No! (Hungarian) - A campaign against online sexual coercion and extortion of children, https://www.youtube.com/watch?v=ufTgIJ2zKTE, letöltés: 2022. január 15.

[448] EUROPOL, Online sexual coercion and extortion is a crime, https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime, letöltés: 2022. január 15.

[449] EUROPOL, Internet Organised Crime Threat Assessment (IOCTA) 2021, https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021, letöltés: 2022. január 15.

[450] European Data Protection Board, Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021 1.0, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf, letöltés: 2022. január 15.

fázison ment keresztül, aminek tudományos, technikai és jogtörténeti vonatkozása is jelentős. Napjainkban az információbiztonság helye és szerepe, irányultsága és kapcsolata más tudományágakkal olyannyira jelentős, hogy ott, ahol az informatika jelen van, ott az adatvédelemnek és az információbiztonságnak is jelentős szerep jut. A történeti, technikai, jogtényezői kapcsolati viszony feltárása és bemutatása lényeges, hiszen egy korban egészen fiatal tudományterületből kifejlődött jogintézmények és technológiák egészen egyedi szimbiózisa. A második fejezetben felsorakoztatott történelmi események, adatvédelmi tendenciák, tudományos álláspontok, alapelvek és szabályozási törekvések azt igazolják, hogy a technológiai megvalósítással egy időben rendre megtörtént az adatvédelmi alapelvek lefektetése, az adatvédelmi és később az információbiztonsági szabályok és rendelkezések megfogalmazása, hatályba lépése. Kutatásom során megállapítottam, hogy az információbiztonsági szabályozás nem terjed ki minden jogi személyre, csak az állami és önkormányzati szervekre. Véleményem szerint a szerzői jogra (2. melléklet, A szellemi alkotások jogtörténete és védelme) vagy az adatvédelemre vonatkozó alapelvek megfogalmazása olyannyira bizonyult hasznosnak és elfogadottnak, hogy azok alkalmazása és azokra épített adatvédelmi és információbiztonsági szabályozási rendszer stabil, és amely fejlesztését (GDPR, Infotv., IBtv.) az információs technológia fejlődése, az Ipar 4.0 folyamata indokolta. A második fejezetben megvizsgáltam a nemzetközi és a hazai adatvédelmi (GDPR, német szövetségi adatvédelmi törvény, Infotv.) és az információbiztonsági rendelkezések (IBtv.) és szabványi ajánlások (ISO/IEC 27001) jelentőségét és az adatvédelmi alapelvek, valamint szabályok alkalmazásának szükségességét, amelyet az adatvédelmi és információbiztonsági jogtörténet vizsgálatánál összegeztem. Az információ védelmére irányuló történeti és adatvédelmi, információbiztonsági jogtörténeti áttekintés során megfogalmazott következtetéseim rámutatnak arra, hogy a vonatkozó alapelvek és rendelkezések megalkotása és alkalmazása indokolt a személyes adatok védelmének biztosításához. A vizsgálatom során megállapítottam, hogy a hazai adatvédelmi (Infotv.) és információbiztonsági (IBtv.) törvényi előírások és rendelkezések összhangban vannak a nemzetközi adatvédelmi rendelkezésekkel (GDPR, német szövetségi adatvédelmi törvény), valamint a nemzetközi információbiztonsági irányítási rendszer (ISO/IEC 27000 szabványcsalád, ISO/IEC 27001, A melléklet) ajánlásával, ugyanakkor a törvények értelmező rendelkezései helyenként nincsenek összhangban, nem teljes, alapszintű meghatározások hiányoznak és a meglévők pontosításra szorulnak, továbbá a következetesség tekintetében elegendő lenne csak az egyik jogszabályban rögzíteni az releváns fogalmakat. Az adatvédelmi fogalmak az Infotv., míg az információbiztonsági meghatározások

az IBtv. hatásköre. Az adatvédelmi és információbiztonsági fogalmak vizsgálata során megállapítottam, hogy a technológiai fejlődéshez mért egységes magyar adatvédelmi és információbiztonsági értelmező rendelkezések fejlesztése szükséges. Szükséges továbbá az adatvédelmi és információbiztonsági vonatkozó szakkifejezések korrelációjának definiálása, mivel ezen megállapítások az adatvédelem és az információbiztonság oktatás alapjai.

Az említett adatvédelmi, információbiztonsági rendelkezések és szabványi ajánlások elősegítik a rendelkezések és szabványi ajánlások intézményi szintű alkalmazását, de a tisztázatlan fogalmak a jogszabályok értelmezését félrevezetik. A megállapítást, kutatásom során megjelentetett publikációk[451] [452] [453] és a 2.4 fejezet együttes értelmezése igazolja. A harmadik és negyedik fejezetben hivatkozott hatóságok által vizsgált esetek, valamint a hivatkozott publikációk statisztikai adatai rámutatnak arra, hogy a rendelkezések, szabványi ajánlások intézményi szintű, együttes alkalmazása kielégíti az információbiztonsági szabályozási igényeket is. A megállapításom ugyan egy adott időszakban mért állapotot mutat. ugyanakkor azt is jelenti, hogy az előírásokat bevezetni, működtetni, fenntartani és fejleszteni a PDCA elvek alkalmazása szerint minden szinten (politikai, jogi, gazdasági, oktatási, egészségügyi stb.) szükséges, ezáltal teljesíthetők az információbiztonsági követelmények is[454]. A kutatásom alapján megállapítom, hogy az információbiztonsági jogszabályi előírások kiterjesztése legalább 250 fő munkavállalót és egyéni vállalkozót foglalkoztató vállalkozásokra szükséges.

A kutatás során megállapítottam, hogy a Magyarországon érvényes adatvédelmi és információbiztonsági vonatkozású jogszabályok alkalmazása hatékonyan befolyásolja az információs társadalom fejlődését. Az érvényben és hatályban lévő adatvédelmi és információbiztonsági szabályok alkalmazása korlátozza az adatgyűjtést, csökkenti az adatvédelmi incidensek számát, növeli az információs rendszerek információbiztonsági szintjét. A szabályok alkalmazásával lehetőség van az adatvédelmi jogsértések szankcionálására. A disszertáció harmadik, negyedik és az ötödik fejezetében felsorakoztatott incidensek és statisztikai adatok igazolják, hogy az adatvédelmi és információbiztonsági

[451] Ferenc, Leitold, Kálmán Hadarics , Eszter Oroszi , Krisztina Győrffy: Measuring the information security risk in an infrastructure, MALWARE 2015 10th International Conference on Malicious and Unwanted Software, Puerto Rico, 2015

[452] Győrffyné Holló Krisztina: Az információbiztonság jelentősége és története, GRADUS Vol 8, No 2 (2021), John von Neumann University, Hungary, Kecskemét

[453] [45.] Krisztina Győrffyné Holló, Adam Karisztl, Domino effect and other models in the IT process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

[454] Krasznay Csaba, Okoseszközök a kritikus információs infrastruktúrákban, Információ- és kiberbiztonság, Fenntartható biztonság és társadalmi környezet tanulmányok V., Sorozatszerkesztő: Kis Norbert, Koltay András, Szerkesztette: Török Bernát, Budapest, 2020. (kiberbiztonsági szempont)

szabályok megalkotása és alkalmazása elengedhetetlen. Az adatvédelmi és információbiztonsági szabályozás egyik jogalapja az adatvédelmi jogsértés. A komplex szabályozási rendszer többcélú lehetőséget nyújt az állampolgároknak, a vállalkozásoknak és az intézményeknek egyaránt. Egyrészt útmutatóul szolgál az információs rendszerek tervezéséhez, fenntartásához és védelméhez, a jogszerű adatkezelés, adatfeldolgozás és adattovábbítás megvalósításához, másrészt a nem jogszerű tevékenységek szankcionálásával elősegíti az állampolgári bizalom kialakulását. Tehát, az adatvédelmi és információbiztonsági szabályok a informatikai technológiai folyamatokkal koherens fejlesztése és alkalmazása állampolgári bizalom erősítő tényező. Az adatvédelmi és információbiztonsági incidensek statisztikai adatai megmutatják, hogy az elmúlt évek alatt a szabályrendszer fejlesztése az Ipar 4.0 okozta technológiai fejlődést megfelelően követte. Kutatásom során megállapítottam, hogy a megalkotott magyarországi szabályok az EU jogalkotói elvárásoknak megfelelő, védelmet nyújtanak az állampolgárok adatai számára, biztosítják az adatvédelmi és információbiztonsági jogokat, egyértelműen rögzítik az adatkezelők és adatfeldolgozók feladatait, jogait és kötelezettségeit, ugyanakkor további fejlesztésre szorul. Kutatásom során megállapítottam, hogy az incidensek egyik legnagyobb tényezője a technológiai megoldásokon túl, a „*humán faktor*”, ezáltal az állampolgárok adatvédelmi támogatása és a bizalmának erősítése az információs rendszer kulcsfontosságú tényezője. A megállapítások a H1 és H2, valamint a H1 és H3 hipotézisek összefüggéseit indirekt és inverz módon is igazolják.

A második hipotézisem (H2) igazolásához a harmadik, negyedik és ötödik fejezetben vizsgált statisztikai adatokat használtam fel, amelyek alátámasztják a „*humán faktor*” jelentőségét, amely az információs rendszerek információbiztonsági szintjének befolyásoló tényezője. Ezen terület fejlesztése erősítő információbiztonsági szintet, míg elhanyagolása csökkenő tendenciát eredményez. A második hipotézisem (H2) szerint tehát feltételeztem, hogy a felhasználói információbiztonsági tudatosság hiánya, amely emberi tévedést és szándékos kárt is eredményezhet, elősegíti az adatvédelmi jogsértések bekövetkezését, ezáltal a kiberbűnözést. A statisztikai adatok rámutatnak arra, hogy a kiberbűnözés jelentős károkat okozott különösen az egészségügyi, oktatási, igazgatási, banki, ipari és egyéb szolgáltatóipari ágazatnak, a helyreállítás és a védelmi szint megerősítése jelentős anyagi ráfordítással járt. A kutatás során megállapítottam, hogy az adatvédelmi eseménybekövetkezési valószínűség függvényében, a „humán faktor” részarány tekintetében a felhasználói információbiztonsági tudatosság hiánya adatvédelmi jogsértéseket eredményez. Az adatvédelmi jogsértések jelentős része kiberbűnözői tevékenység. Tehát a H2 hipotézis során igazolt inverz és közvetett megállapítás szerint az

információbiztonsági tudatosság fejlesztése kiberbűnözői tevékenység csökkentő tényező. Következtetésként megállapítom, hogy tekintettel az incidensek „humán error” tényezőire a preventív információbiztonsági folyamatok erősítésének érdekében komplexebb adatvédelmi és információbiztonsági tudatosítás szükséges. A fenti megállapításokkal a H2 és H3 valamint a H2 és H4 ok-okozati összefüggéseit igazoltam.

A harmadik hipotézisem (H3) szerint feltételeztem, hogy a Magyarországon érvényes és intézményi adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését és a szervezet információbiztonsági tudatosság szintjét. Erre a hipotézisre a harmadik, negyedik és ötödik fejezet ad választ, amelyet az ENISA által feldolgozott statisztikai adatokkal és a szervezet által hivatkozott tanulmányokkal lehet igazolni. Az ENISA felmérésében részt vettek az Európai Unió országainak képviselői, amely nemcsak Uniós országok adatait, hanem a világszinten elérhető, tudományos cikkek kutatási adatait tartalmazza. Saját kutatási adataimat is felhasználva igazoltam azt a felvetést, miszerint az adatvédelem jelentőségének tudatosítása és az információbiztonsági tudatosság fejlesztése csökkenti az emberi hiszékenység kihasználását, a tévedések, mulasztások és szándékos károkozás számát, ezáltal is erősíthető a szervezet információbiztonsági szintje. Egy-egy információbiztonsági kurzus felnőttek részére 3-5 nap is lehet, amikor továbbképzés formájában adatvédelmi alapelveket, szabályozási kötelezettségeket és lehetőségeket, információbiztonsági alapelveket, kockázatkezelést, információbiztonsági szabályozási kötelezettségeket és lehetőségeket, valamint auditori képességeket sajátíthatnak el az érintettek (CISA, CISM, ISO/IEC 27001, Kockázatkezelés, belső és vezető auditori képzések). A felsőoktatás, mint például az Eötvös Loránd Tudományegyetem, Jogi Továbbképző Intézete által indított Adatbiztonsági és adatvédelmi jogi szakokleveles szakember vagy az Adatbiztonsági és adatvédelmi szakjogász képzés[455] [456], illetve a Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet által szervezett Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak vagy az Elektronikus információbiztonsági vezető szakirányú továbbképzési szak[457] által biztosított, jogász, illetve

[455] ELTE Jogi Továbbképző Intézet, Adatbiztonsági és adatvédelmi jogi szakokleveles szakember képzés, https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-jogi-szakokleveles-szakember.t.562, letöltés: 2022. július 29.

[456] ELTE Jogi Továbbképző Intézet, Adatbiztonsági és adatvédelmi szakjogász, https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406, letöltés: 2022. augusztus 2.

[457] Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, Digitális térségfejlesztés szakirányú továbbképzési szak, Integritás tanácsadó szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/altalanos-informaciok,

felsőfokú adatvédelmi és információbiztonsági vezetői és intézményi alkalmazottak részére nyújtott továbbképzés[458], lehetőség ad a közszolgálati és más intézmények munkavállalóinak az aktuális, magas szintű adatvédelmi és információbiztonsági alapelvek, szabályok,[459] valamint gyakorlati megoldások elsajátítására.[460] A felsőoktatási intézmények által szervezett informatikai alapképzéseken és szakirányú továbbképzéseken elsődlegesen biztonságtechnikai, kiberbiztonsági megoldásokat tanulhatnak a fiatalok.[461] Véleményem szerint ez az irány megfelelő és a jövőben tartani szükséges, ugyanakkor az értekezés harmadik, negyedik és ötödik fejezetében bemutatott kutatásom statisztikai adatai és tanulmányaim rámutatnak arra, hogy az információbiztonsági tudatosításra fordított idő és tevékenység nem elegendő a gyermekek körében. A gyermekek képesek arra, hogy egy új digitális eszköz lehetőségeit feltérképezzék, mindezt használati útmutató nélkül, sok esetben egymástól eltanulva vagy autodidakta módon. Véleményem szerint az évi 3-4 alkalom kevés arra, hogy a megfelelő adatvédelmi és információbiztonsági képességeket elsajátítsák.

A negyedik hipotézisem (H4) szerint feltételeztem, hogy az információbiztonsági tudatosítás rendszerét nemcsak az informatikai oktatásban, hanem minden korosztály számára elérhetővé kell tenni és minden szakterületen indokolt bevezetni és működtetni. A harmadik, negyedik és ötödik fejezetben található elméletekkel, statisztikai adatokkal és következtetésekkel igazoltam, ahogy az informatikai technológia is fejlődik, az adatvédelmi és információbiztonsági incidensek száma évről-évre növekszik, és a hazai adatvédelmi és az információbiztonsági rendelkezések ezt a folyamatot megfelelően lekövetik, tehát szintén intenzív fejlődést mutat, ami az Infotv. (2011., 2018.), IBtv. (2013.) és a GDPR (2016.) megjelenésével igazolható. Az elmúlt tíz év kutatás adatai (ötödik fejezet) és az ENISA 2017. évi tanulmánya rámutat arra,

---

Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok, letöltés: 2022. január 17.

[458] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

[459] Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/tananyagok

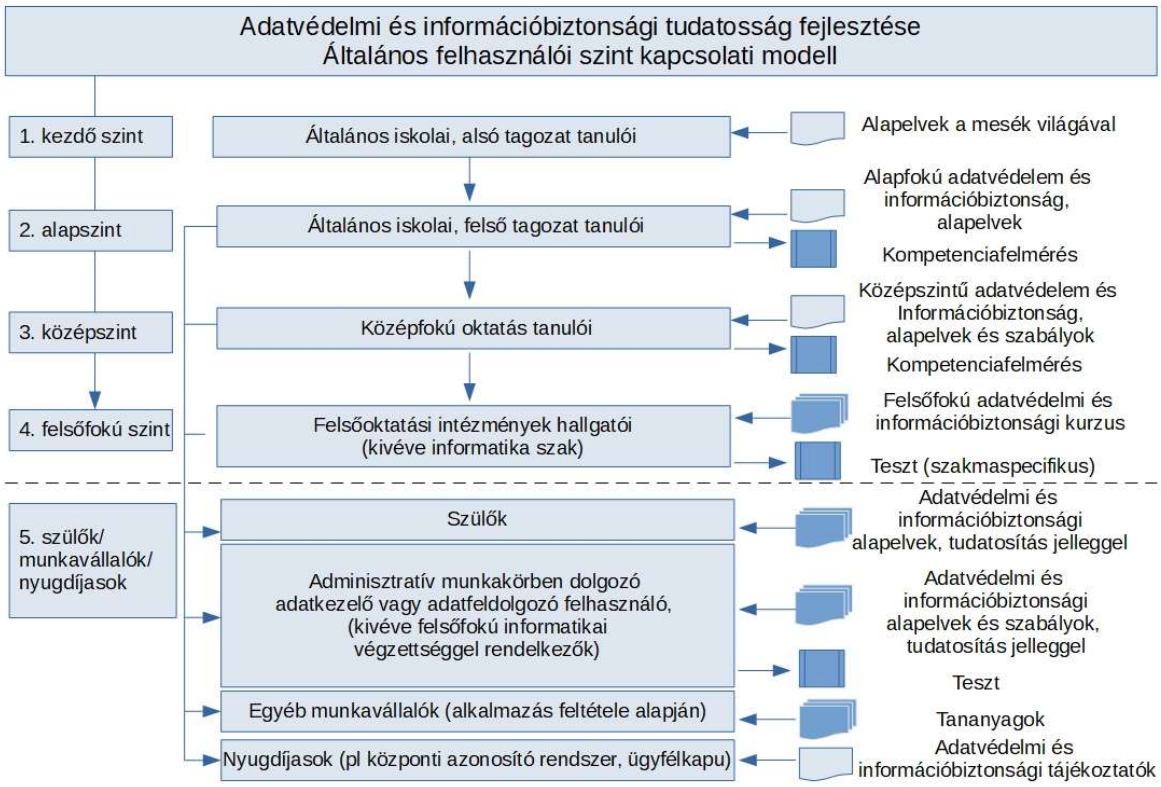
[460] Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, Elektronikus információbiztonsági vezető szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/tananyagok

[461] Felsőoktatási képzések, Óbudai Egyetem, Neumann János Informatikai Kar, https://nik.uni-obuda.hu/kepzesek/
Neumann János Egyetem, GAMF Műszaki és Informatikai Kar, https://gamf.uni-neumann.hu/kepzeseink/
Miskolci Egyetem, Gépészmérnöki és Informatikai Kar, https://www.iit.uni-miskolc.hu/oktatas.html
Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar, https://www.vik.bme.hu/oktatas/
Pannon Egyetem, Műszaki Informatikai Kar, https://mik.uni-pannon.hu/index.php/hu/felveteli-menu/felveteli-a-mik-en.html, letöltés: 2022. január 18.

hogy a digitális kompetenciafejlesztés (DigComp 2.0 – 2016., DigComp 2.1 – 2017., DigComp 2.2 felhívás: 2022.) igénye és legfőképp gyakorlata messze elmarad a technológiai és szabályozási törekvésektől, tehát információbiztonsági oktatási módszerek kidolgozása és alkalmazása lassabb fejlődést mutat. Az Oktatási Hivatal, Digitális Pedagógiai Fejlesztések Munkacsoportja 2021. tavaszán hozta nyilvánosságra *A DigComp 2.1 EU-ajánlás alapján kidolgozott javaslat a tanulók digitáliskompetencia-szintjeinek meghatározásához és fejlesztéséhez* című ajánlását. A ötödik fejezetben összegzett kutatási adatok rámutatnak arra, hogy az emberi hibák és következmények száma csökkenthető az információbiztonsági tudatosság fejlesztési rendszer bevezetésével. A digitális technológiák dinamikus fejlődése miatt a digitális kompetenciák fejlesztése elengedhetetlen, az ezzel kapcsolatos döntéseket, a fejlesztések alkalmazását támogatni szükséges, és elérhetővé kell tenni minden korosztály, de legfőképp a felhasználóink – különösen a KRÉTA és iskolai hálózat, valamint elektronikus tankönyvek használói, tehát az általános iskolák és középfokú intézmények tanulói – számára. Kutatásom során megállapítottam, hogy a gyerekek, és az átlag, nem informatikai szakterületen tanult, felsőfokú szakképesítéssel nem rendelkező felhasználók (5+1 szint: Általános felhasználói szint[462]) számára is biztosítani kell a megfelelő szintű és óraszámú digitális, adatvédelmi és információbiztonsági képzéseket, az alábbi ábrán szereplő szintek alapján, úgymint az érintett felhasználói kör számára, a figyelembe vehető input, tudatosítási eszközök és az output információbiztonsági tudatossági szint meghatározásához szükséges digitális kompetencia felmérési folyamatok alkalmazásával.

A hipotézisek igazolása alapján meghatároztam az adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó általános felhasználói szint kapcsolati modellt (23. ábra), amely alapján 5 szintet különítettem el. Az első négy szint általános iskolai, középszintű és felsőoktatási intézmények tanulói és hallgatói által, lehetőleg meglévő tantárgyak (digitális kultúra, informatika alapjai, adatbiztonság és adatvédelem) keretén belül igénybe vehető adatvédelmi és információbiztonsági tudatosítási módszerek alapján kidolgozott tananyagok segítségével elsajátíthatják az aktuális alapelveket és szabályokat, trendeket.

[462] Mádi-Nátor Anett, Kardos Zoltán, Nemzeti Közszolgálati Egyetem, Mádi-Nátor Anett, Kardos Zoltán, Információbiztonság-tudatosság gyakorlat, Nemzeti Közszolgálati Egyetem, https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsag-tudatossag-gyakorlat.original.pdf, letöltés: 2022. január 18..



23. ábra, az adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó általános felhasználói szint kapcsolati modell, saját szerkesztés

Az ötödik szinten, az adminisztratív munkakörben foglalkoztatott, adatkezelő vagy adatfeldolgozó munkavállalók - különösen elektronikus ügyintézés[463] - esetében a tudatosság fejlesztését, elsődlegesen közigazgatási, államigazgatási, illetve legalább 250 fő munkavállalót foglalkoztató szervezetek tekintetében javasolt megvalósítani. Végül azon nyugdíjasok vagy felnőttek (máshová nem besorolható, különösen nem vezető, nem adminisztratív munkakörben dolgozók vagy informatikai végzettséggel rendelkezők) körét sem szabad kihagyni, akik leginkább a központi azonosító, ügyfélkapu, elektronikus ügyintézés vagy egyéb szervezet, például bank információs rendszeréhez kapnak hozzáférést. Ugyanakkor szeretném

[463] elektronikus ügyintézési szolgáltatás például biztonságos kézbesítési szolgáltatás (BKSZ), kézbesítési szolgáltatás, (KSZ), elektronikus aláírással kapcsolatos szolgáltatás, (KEAESZ - mint a Kormány által nyújtott hitelesítési szolgáltatás része), ügyfél ügyintézési rendelkezésének nyilvántartása (RNY), iratérvényességi nyilvántartás (IÉNY), ügyfél időszaki értesítése az elektronikus ügyintézési cselekményről (RÉR), összerendelési nyilvántartás (ÖNY), részleges kódú telefonos azonosítás (RKTA), elektronikus fizetési és elszámolási rendszer (EFER), kormányzati hitelesítés- szolgáltatás (GovCA), központi azonosítási ügynök (KAÜ), ÁNYK űrlapbenyújtás támogatási szolgáltatás (ÁBT), ügyfélkapu elektronikus tájékoztatási szolgáltatás, azonosításra visszavezetett dokumentumhitelesítés (AVDH), elektronikus irat átalakítása hiteles papír alapú irattá (HIBRID), papír alapú irat átalakítása hiteles elektronikus irattá (INVERZ HIBRID)

hangsúlyozni, hogy az értekezés ezen felhasználói rétegével nem foglalkozik. Az adatvédelmi és információbiztonsági képzések hiányában az érintettek megfelelő szintű digitális kompetenciát nem szerezhetnek, ami nagymértékű információbiztonsági tudatossági hiányt okoz (H2 hipotézis vonatkozásai), ezáltal magas kockázati tényezőt jelent. Az adatvédelmi és információbiztonsági alapelvek közvetítése minden korosztály számára, és minden szakterületen fontos, hiszen a számítógépeket, mobiltelefont, szoftvereket és adatbázisokat, nemcsak az informatikusok és nemcsak az informatikai szakterületen használják, tehát mindenkinek rendelkezni kell az alapvető adatvédelmi kompetenciával, csak így biztosítható a felhasználói információbiztonsági tudatosság hatékonyan fejlődése.

6.1.2. TUDOMÁNYOS EREDMÉNYEK ÖSSZEGZÉSE

Az értekezés a hazai információbiztonsági tudatosság helyzetére, a hiányának sajátosságaira, azok következményeire és pótlásának lehetőségeitre fókuszálva vizsgálta, különösen az adatvédelmi és információbiztonsági aspektusait, fogalomkörébe tartozó jogintézmények és tényezők összefüggéseit, jogsértések kockázatait és kockázatcsökkentő tényezőit, az információbiztonsági kockázatkezelés alapján meghatározható hazai adatvédelmi és az információbiztonsági tudatosítási folyamatot és összetevőket. Az értekezés szerkezeti struktúrája leköveti az európai és hazai adatvédelmi és az információbiztonsági történeti és szabályozásának vonulatát, a biztonságtudatosság kutatási területéből, különös tekintettel az adatvédelmi, információbiztonsági és az információbiztonsági tudatosság helyzetéből kiindulva jut el az adatvédelmi és információbiztonsági rendelkezések és a digitális kultúra, különösen az általános felhasználói szint fejlesztésének igényéig. Az előbbiek tekintetében tisztáztam az adatvédelmi és az információbiztonsági jogtényezők viszonyát, a fogalomrendszer tényezőit. A második fejezetben szereplő fogalommeghatározások alapján kialakíthatók a letisztult, egységes, értelmező rendelkezések meghatározásai, annak érdekében, hogy a társadalom szereplői számára egyértelműbb rálátást biztosítsanak, ezzel biztosítva az adatvédelmi és információbiztonsági alapelvek tudatosítását, javítva a tudatosítási folymatok minőségét, hatékonyságát és a visszacsatolási folyamatok eredményeinek szintjét. Kutatási eredményemként bemutatott adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó általános felhasználói szint kapcsolati modell ezen folyamtok megvalósításának alapjául szolgálhat. A visszacsatolás jelentőségének tekintetében megállapítottam, hogy a visszacsatolás hiánya is jelentésértékű, ami bizonytalan végeredményeket, akár téves értékelést

és kevésbé reális, „tényeken alapuló döntéshozatalt”, az erre épített intézkedéseket beleértve, meghatározó mértékben befolyásolja, tehát jelentős kockázati tényező.
Az értekezés részösszefoglalásainak és a hipotézisek igazolása alapján eredményeimet az alábbiakban összegzem.

A H1 hipotézis összefüggésében az adatvédelmi, információbiztonsági jogtörténeti áttekintés során megfogalmazott következtetéseim rámutatnak arra, hogy a vonatkozó alapelvek és rendelkezések megfogalmazása és megalkotása és alkalmazása indokolt a személyes adatok védelmének biztosításához. A vizsgálat során megállapítottam, hogy a hazai adatvédelmi és információbiztonsági előírások és rendelkezések összhangban vannak a nemzetközi adatvédelmi rendelkezésekkel, az általános adatvédelmi rendelettel, valamint a német szövetségi adatvédelmi törvény vonatkozó meghatározásaival, valamint a nemzetközi információbiztonsági irányítási rendszer ajánlásaival, ugyanakkor a törvények értelmező rendelkezései helyenként nincsenek összhangban, meghatározó szakkifejezések deklarálása hiányozik és a meglévők erőteljes pontosításra szorulnak, továbbá a következetesség tekintetében a redundáns fogalommeghatározás javítása szükséges. Az adatvédelmi fogalomkörébe tartozó értelmezések az Infotv., az információbiztonsági és kibervédelmi meghatározások az IBtv. hatásköre, tehát a tudomány mai álláspontja szerint lekövetett, egységes magyar adatvédelmi és információbiztonsági értelmező rendelkezések beiktatása szükséges, a vonatkozó szakkifejezések korrelációjának definiálásával. Tekintettel arra, hogy az IBtv. nem terjed ki minden jogi személyre, csak az állami és önkormányzati szervekre, ezért a magyarországi információbiztonsági szabályozás hatálya terén jelentős hiányosság tapasztalható, tehát az információbiztonsági jogszabályi előírások kiterjesztése legalább 250 fő munkavállalót és egyéni vállalkozót foglalkoztató vállalkozásokra szükséges. Megállapítottam továbbá, hogy az állampolgárok adatvédelmi és információbiztonsági előírások általi támogatása és tudatosítása állampolgári bizalom erősítő, valamint humán faktor befolyásoló, közvetett módon kockázatcsökkentő tényező (H1 és H2, valamint H1 és H3 hipotézisek összefüggései).

A H2 hipotézis összefüggésében megállapítottam, hogy az adatvédelmi eseménybekövetkezési valószínűség függvényében, a „humán faktor”, de különösen a „humán error” részarány vonatkozásában a felhasználói információbiztonsági tudatosság hiánya adatvédelmi jogsértéseket eredményez, amelynek jelentős hányada kiberbűnözői tevékenység, továbbá az információbiztonsági tudatosság fejlesztése kiberbűnözői tevékenység csökkentő tényező. A preventív információbiztonsági folyamatok hatékonysága érdekében komplexebb adatvédelmi

és információbiztonsági tudatosítás szükséges. (Adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó általános felhasználói szint kapcsolati modell, H2 és H3 hipotézisek összefüggései.)

A H3 hipotézis összefüggésében megállapítottam, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését, ugyanakkor az adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó általános felhasználói szint kapcsolati modellel összefüggésben a tudatosítási és visszacsatolási folyamatok további erősítése, fejlesztése szükséges.

A H4 hipotézis összefüggésében megállapítottam, hogy az információbiztonsági tudatosítás rendszerét nemcsak az informatikai oktatásban, hanem minden korosztály számára elérhetővé kell tenni és minden szakterületen indokolt bevezetni és működtetni. A megfelelő szintű (adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó általános felhasználói szint kapcsolati modell) adatvédelmi és információbiztonsági képzések hiányában az érintettek elvárt szintű digitális kompetenciát nem szerezhetnek, ami számottevő információbiztonsági tudatossági hiányt okoz (H2 hipotézis összefüggése). Az adatvédelmi és információbiztonsági alapelveket minden korosztály számára elérhetővé kell tenni, mivel mindenki, de legfőképp az általános felhasználói szinten lévő felhasználók számára, csak így biztosítható a felhasználói információbiztonsági tudatosság hatékonyan fejlődése, ezáltal a digitális kompetencia a technikai fejlődést követő, megfelelő ütemű fejlődése.

6.2. JAVASLATOK AZ ÚJ TUDOMÁNYOS EREDMÉNYEK HASZNOSÍTÁSÁRA ÉS FELHASZNÁLÁSÁRA

Gyakorlati felhasználhatóságát tekintve a dolgozat lehetőséget teremt az információbiztonsági tudatosság fejlesztésére irányuló képességfejlesztések alkalmazására minden korosztály számára. Az alábbiakban kiemeltem az óvodás korú gyermekek és a szülők digitális képességének fejlesztésére irányuló javaslataimat, tekintettel arra, hogy az általános és a középiskolákban digitális kultúra (informatika) oktatás keretében, az óraszámelosztást igazítva az aktuális igényekhez, a tematikákat a tudatosításra vonatkozó módszerekkel és tananyagokkal (adatbiztonság, adatvédelem, információbiztonság, kibervédelem, kiberbiztonság alapjai, alapelvek, magatartási kódex – IB képzés) lehetne kibővíteni. A felsőfokú képzésekben (felsőoktatási szakképzés, főiskolai, BSc, MSc, szakirányú továbbképzés) minden képzési szint számára biztosítani kell az igény és szükség szerinti információbiztonsági tudatosítás

tananyagait. Az igény vagy szükség szerinti IB képzés meghatározója lehet a felvételi alkalmával a leendő hallgatók által kitöltött IB tesztek eredményei. Ezáltal akár helyi szinten, kompetenciának megfelelően biztosítható az IB képzés.

6.2.1. INFORMÁCIÓBIZTONSÁGI TUDATOSÍTÁSI JAVASLATOK ÓVODÁS KORÚ GYERMEKEK SZÁMÁRA

Napjainkban egyre nagyobb figyelmet kap a gyermekek kiberbiztonsága, és ennek köszönhetően az információbiztonsági tudatosság növelése, a gyermekek különböző online fenyegetéseknek való kiszolgáltatottsága és kockázatok vizsgálata.[464] Informatikus és nem informatikai végzettséggel rendelkező szülők, pedagógusok és szakemberek körében is vitatott téma a 10 év alatti gyermekek számára az információbiztonsági tudatosítás módszereinek alkalmazása, ugyanakkor napi szinten tapasztalhatjuk, hogy a szülő, akár a pár éves gyermekének is odaadja okostelefonját, Tabletét, figyelemelterelés vagy szórakoztatás, pl. filmnézés célzattal. Természetesen pár éves gyermek esetében nehéz lenne elmagyarázni a biztonságtudatosság elveit és szakkifejezéseit, mivel csupán a zenék, a változó alakok, színes képernyő az, ami magával ragadja a csöppségeket. A négy-hét éves gyermekeket, akik már értik a mese világát be lehet avatni a biztonság, a csúnya-szép, a rossz-jó világába, legyen az internet, egy alkalmazás, vagy a *Piroska és a farkas*, illetve az *Öreg néne őzikéje* meséje. Amennyiben elfogadjuk, hogy a gyermek ösztönösen különbséget tud tenni jó és rossz között, és a mesék által tanítható, úgy a digitális képességek játékossággal és tanmesékkel, gyermeki szinten is taníthatók. Az alábbi készségfejlesztési területek lehetnek digitális eszközökkel:

- hálózat és kapcsolatok, akár egy társasjátékkal,
- tartalomkészítés, digitális rajztáblákkal,
- virtuális interakciók, memóriajátékok és online páros játékok,
- internethasználat, okostelefon használata.

Az alábbi praktikákat javaslom a tudatosítási módszer kidolgozásához:

- Legyen játékos, izgalmas és szórakoztató, ugyanakkor gondolkodásserkentő, akár a Legoval való játék, folyamatos interakcióval. Az okosjátékok (smart toy), amely már elérhető a baby játékoktól az okostabletig (smart tablet), valamint a tanuló okostelefonig, vagy a mechanikus és digitális megoldásokat együttesen alkalmazó játékokig, közelebb

[464] Farzana Quayyum, Daniela S. Cruzes, Letizia Jaccheri, Cybersecurity awareness for children: A systematic literature review, International Journal of Child-Computer Interaction, Volume 30, 2021.

viszik a gyermekeket a digitális világhoz, egyben felkészíti őket az saját telefon használatára.

- Szógyűjtés, memorizálás, azonosítás a „mit visz a kishajó?” és „a nap szava” vagy a „szuperhős” koncepció játékos lehetőséget adhat a szakszavak gyűjtésére és memorizálására. A titkos, 007-es ügynökakció erősíti az azonosítás (identifikáció), az identitás, az egyedi, a védelem, a biztonság kifejezések megalapozását.
- A kreativitás, a megosztás, a védelem szakkifejezések például homokvár építés során is előkerülhetnek, hiszen a várépítés csapatban, a kislapátok kölcsönadása vagy megosztása, bástya védelmének kialakítása és megszilárdítása, a hős várkapitány a védelem megtestesítője, az ismeretlen helyről érkező küldönc leveleinek nem fogadása, új kereskedők termékeinek átvizsgálása, és a homokvár biztosítása eső ellen, mind információbiztonsági szakkifejezést erősítő megoldás lehet.
- CIA alapelvek tanítása, akár a rajzfilmek, mesék olvasása által is lehetséges. Az olyan mesék, mint például a *Piroska és a farkas*, *Csipkerózsika*, *A kristálygolyó* (Grimm) erősítik a kitartás (királyfi), a hatás (varázsló átka), a védelem (harmadik fiú), személyiséglopás (farkas), a kiberbűnöző (farkas) fogalmának kialakulását. A bizalom a varázseszközök iránt (varázskalap), titkosítás és védelem (rózsasövény), rendelkezésre állás (sas), sértetlenség (boszorkány varázslata) szakkifejezések megértését. Ezen kívül megmagyarázható az internet világa a varázskalap szimbólumának használatával. A mesék erősítik az ismeretlen iránti egészséges bizalmatlanság kialakulását, például az előugró ablakok és ismeretlen reklámok esetében (Piroska, ne állj szóba idegenekkel! Ne térj le az útról!), az erkölcsi iránytűt vagy az őszinteséget.

A játék során használt szimbólumok párosítása a szakkifejezésekkel elsegítheti az információbiztonsági alapelvek megértését.

- Információbiztonsági koncepció – iskolakezdők részére:
    - identitásvédelem – csak egy kattintás is végzetes lehet,
    - mentés – digitális rajzok mentése,
    - segítség kérés és elfogadás képesség kialakítása,
    - kiberfenyegetések – akár a közlekedésben,
    - nem hiteles tartalom – ahogy a rossz ízű ételt sem esszük meg,
    - egészséges, digitális világ iránti kíváncsiság fejlesztése,
    - „A te játékod, te vagy a gazdája” – jó gazda szemlélet kialakítása a digitális térben,
    - kiberlábnyom tudatosítása.

A fenti javaslatok alkalmazása óvodai környezetben jobban érvényesül szakemberek, óvodapedagógus támogatásával. A szülők bevonása is feltétlen szükséges, mivel ők azok, akik okostelefont adnak az elsős, másodikos kisiskolásnak, a folyamatos kapcsolattartás érdekében.

6.2.2. INFORMÁCIÓBIZTONSÁGI TUDATOSÍTÁSI JAVASLATOK SZÜLŐK SZÁMÁRA

Tekintettel arra, hogy a szülők figyelemmel kísérik gyermekük tanulmányait, célszerű csoportos, szülői értekezletek alkalmait felhasználni az információbiztonsági tudatosítás eszközeit. Témák lehetnek:

- Adatvédelmi alapelvek iskolai példákkal,
- CIA alapelvek iskolai példákkal,
- Esettanulmányok,
- Tanulás támogatása okoseszközökkel.

6.3. ZÁRÓ GONDOLATOK

Az informatikai technológiák, valamint az információs társadalom fejlődése, digitális kompetenciák fejlesztése és az adatvédelmi és információbiztonsági szabályozási rendszer hatással van egymásra. Ezen összefüggések információbiztonsági mérése lehetőséget ad az empirikus, szubjektív következtetések összegzésére és a statisztikai adatok értékelésére. A disszertációban bemutatásra kerültek a kutatás szempontjából releváns módszerek, adatvédelmi, kiberbűnözési, valamint a digitális kompetencia állapotát mutató statisztikai adatok, amelyekkel a hipotéziseket kívántam igazolni. Kutatásomat jelentősen segítette a BSC stratégiai módszertan is. A stratégia jellegű felméréshez és a kiértékeléshez egyik jól használható módszer a Balanced Scorecard (1. számú melléklet). A módszert elsősorban az információbiztonsági intézkedési tervek elkészítéséhez, kockázatfelmérési és –elemzési stratégiához, a háttérkutatáshoz és –elemzéshez használtam fel, ugyanakkor nem része az értekezésnek. Az értekezésben kapott eredmények alkalmasak a kutatás továbbfejlesztésére, az információbiztonsághoz kapcsolódó stratégiai térkép megalkotására, a gyermekek biztonságtudatos gondolkodásának fejlesztésére irányuló módszerek kidolgozására, az IBtv. kiterjesztésére legalább 250 fő munkavállalót foglalkoztató vállalatokra, valamint a magatartási kódex megalkotására a közigazgatásban. Információbiztonsági felméréssel megállapítható az információs rendszer biztonsági szintje és elemezhető a biztonságtudatos magatartás. Az emberi akaratlagos vagy akaraton kívüli magatartásból eredő kár az információbiztonsági

kockázatkezelés módszereivel kimutatható, és hatása, valamint nagysága mérhető. Az emberi magatartás többféle módszerrel befolyásolható. Az információbiztonsági tudatosságot befolyásoló tényező lehet az informatikai technológia és infrastruktúra, az Internet és a rendelkezésre álló információ, a digitális kompetencia, a pszichológiai megtévesztés, a felhasználói közreműködést igénylő fenyegetések és támadások, a kockázatmenedzsment intézkedések. A hipotézisek igazolására szolgál az értekezésben hivatkozott tanulmányok elemzése és a statisztikai adatok összegzése, az adatvédelmi incidensek elemzése és a kimutatások összevetése, valamint ezek összehasonlítása saját információbiztonsági kockázatkezelés által kapott kutatási eredményeimmel. A hipotézisek kifejtéséhez és a kérdések megválaszolásához elengedhetetlenül szükséges az adatvédelmi alapelvek kialakulásának bemutatása, a nemzetközi és a hazai adatvédelmi jogtörténet, valamint az információbiztonság fogalomrendszerének, jogintézményének, környezetének és kapcsolódó történeti tényezők vizsgálata. Az adatvédelmi és információbiztonsági jogtörténeti áttekintés előkészíti a hipotézisigazolásokat és segítséget nyújt a mai szabályok értelmezésében, az adatvédelmi jogsértések valamint az információbiztonsági incidensek elemzéséhez és a következtetések meghatározásához. Az értekezésem végeredményéül kapott állításokkal erősíteni szeretném azt a feltevést, hogy az adatvédelmi és információbiztonsági alapelvekre épített felhasználói információbiztonsági tudatosság növelése nagymértékben hozzájárul az információs rendszereink – és ebben az esetben legfőképp a hazai közszolgálati rendszerek – megerősítéséhez, míg a hiánya vagy gyengesége az információs rendszereink gyenge pontjait növeli, ezáltal az információs rendszer sérülékenyebbé, kihasználhatóbbá válhat. Az értekezésben ismertetett adatvédelmi és információbiztonsági incidensek, valamint azok elemzései, a következtetések igazolják a rendeletekben és törvényekben, valamint egyéb rendelkezésekben szükségszerűen megfogalmazott adatvédelmi és információbiztonsági alapelveket és előírásokat.

FELHASZNÁLT IRODALOM

[1.] A szerzői jog gyakorlati kérdései, Válogatás a Szerzői Jogi Szakértő Testület szak véleményeiből (2010 –2013) fennállásának 130. év fordulója alkalmából, Szellemi Tulajdon Nemzeti Hivatala, Szerkesztő: LEGEZA Dénes, Felelős kiadó: dr. BENDZSEL Miklós, 2014.

[2.] BOYTHA György: A szellemi alkotások joga és az új Ptk., Polgári Jogi Kodifikáció, 2000/2., 46-56. o., Budapest, 2000.

[3.] BELL, Daniel: Az információs társadalom társas keretrendszere, Információ és távközlés a posztindusztriális társadalomban, Információs Társadalom, I., Budapest, 2001 (fordította: Rédey Szilvia, Földvári Balázs)

[4.] BELLA Tamás, A kutatási módszer és mintavétel megválasztása a tudományos kutatásokban, A magyar természettudományi társulat tudománytörténeti kötetei II., pp. 247-263.o., DOI 10.23716/TTO.22.2018.18, Budapest, 2018.

[5.] BERNÁRD Aurél, TÍMÁR István: A szerzői jog kézikönyve. Közgazdasági és Jogi Kiadó, Budapest, 1973.

[6.] Brian DAIGLE, Mahnaz KHAN, The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities, Journal of International Commerce and Economics, 2020.

[7.] BODÓ Attila Pál: Információbiztonsági jogi ismeretek vezetőknek, Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[8.] BUDAI Balázs Benjámin, TÓZSA István: E-közigazgatás, Debrecen, 2007

[9.] CASTELLS, Manuel: Az információ kora. Gazdaság, társadalom és kultúra, trilógia, A hálózati társadalom kialakulása, 1996., Az identitás hatalma, 1997., Az évezred vége, 1998.

[10.] CZUNI László, Biometria a számítógépes személyazonosításban - vizuális módszerek, egyetemi jegyzet, Pannon Egyetem, Műszaki Informatikai Kar, 2015.

[11.] Eszter OROSZI , Krisztina GYŐRFFY: Information security for egovernment social media marketing and citizen interaction, Central and Eastern European eIDem and eIGov Days 2016: Multi-Level (e)Governance: Is ICT a means to enhance transparency and democracy?, Budapest, 2016.

[12.] Farzana QUAYYUM, Daniela S. CRUZES, Letizia JACCHERI, Cybersecurity awareness for children: A systematic literature review, International Journal of Child-Computer Interaction, Volume 30, 2021.

[13.] Ferenc, LEITOLD, Kálmán HADARICS , Eszter OROSZI , Krisztina GYŐRFFY: Measuring the information security risk in an infrastructure, MALWARE 2015 10th International Conference on Malicious and Unwanted Software, Puerto Rico, 2015

[14.] Ferenc LEITOLD, Krisztina GYŐRFFYNÉ HOLLÓ, Zoltán KIRÁLY, Quantitative metrics characterizing malicious samples, In: Cyril, Onwubiko; Pierangelo, Rosati; Aunshul, Rege; Arnau, Erola; Xavier, Bellekens; Hanan, Hindy; Martin Gilje, Jaatun (szerk.) Cyber Science, CyberSA for Trustworthy and Transparent Artificial Intelligence (AI), Dublin, Írország: Center for Multidisciplinary Research, Innovation and Collaboration 2021. pp. 82-83., 2 p.

[15.] FICHTE: Beweis der Unrechtmäßigkeit des Büchernachdrucks. Berliner Monatsschrift, Vol. 21., 1793.

[16.] FORRAI Gábor: A jelek tana: Locke ismeretelmélete és metafizikája, L'Harmattan, Budapest, 2005.

[17.] FÜLÖP Géza: Az információ, 2. bővített és átdolgozott kiadás, Budapest, 1996.

[18.] FÜLÖP Géza: Olvasók, könyvek, könyvtárak. A kezdetektől 1848-49-ig. I. kötet. A könyvnyomtatás feltalálása, Gutenberg. Magyar Médiapedagógiai Műhely, Budapest, 1993

[19.] GÉMES Csaba: Az információbiztonság alapkérdései, Hadmérnök (XII) IV, Budapest, 2017

[20.] GYŐRFFYNÉ HOLLÓ Krisztina: Az információbiztonság jelentősége és története, GRADUS Vol 8, No 2 (2021), John von Neumann University, Hungary, Kecskemét

[21.] GYŐRFFYNÉ HOLLÓ Krisztina, Információbiztonság, avagy incidens kontra biztonságtudatos viselkedés, INFOKOMMUNIKÁCIÓ ÉS JOG 18., 76 pp. 17-23. 7 p., 2021.

[22.] GYŐRFFYNÉ HOLLÓ Krisztina, Az érintés nélküli adatgyűjtés kockázatai és a kockázatszámítás módszerei, DUNAKAVICS 9 : 8 pp. 77-97. , 21 p., 2021.

[23.] GYŐRFFYNÉ HOLLÓ Krisztina, Közszolgálati információs rendszerek interoperabilitási nehézségeinek megoldása, DUNAKAVICS 2021. IX. évfolyam II. szám pp. 21-40. , 19 p., 2021.

[24.] GYŐRFFYNÉ HOLLÓ Krisztina, LEITOLD Ferenc: Felhasználókkal kapcsolatos információbiztonsági intézkedések kezelése a GDPR tükrében, Hétpecsétes történetek 2,5 - a GDPR antológia, Budapest, 2018.

[25.] GYŐRFFYNÉ HOLLÓ Krisztina, Az információbiztonsági sebezhetőségek tényezőinek vizsgálata: A „humán faktor", In: VÁRALJAI, Mariann (szerk.) INFORMATIKA KORSZERŰ TECHNIKÁI KONFERENCIA 2021 „Jövőformáló tudomány" „Fenntarthatóság és digitalizáció" Dunaújváros 2021. november 9.: DUE Press (2021) 80 p. p. 40

[26.] GYŐRFFYNÉ HOLLÓ Krisztina, Információbiztonság, avagy megéri kockáztatni? In: NAGY, Bálint; KATONA, József AZ INFORMATIKA KORSZERŰ TECHNIKÁI KONFERENCIA 2020 : Jövőformáló tudomány programfüzet és absztraktkötet Dunaújváros, 2020. november 9-10., Dunaújváros, DUE Press 2020. 48 p.p. 22

[27.] GYŐRFFYNÉ HOLLÓ Krisztina, Az információbiztonsági tudatos viselkedés az incidensek elkerülésének egyik tényezője, DUNAKAVICS 8 : 12 pp. 5-18. , 14 p. 2020.

[28.] HADARICS, K., GYORFFY, K., Nagy, B., BOGNAR, L., ARROTT, A., LEITOLD, F., Mathematical Model of Distributed Vulnerability Assessement, Security and Protection of Information 2017, University of Defence, IDET BRNO, Czech Republic, 2017

[29.] HALÁSZ Iván, Wenzel Gusztáv és a magyar jogi komparatisztika kezdetei, Pro publico bono - Magyar közigazgatás 3. sz., 2015. 152-162. oldal (összehasonlító jogtörténet)

[30.] H.W. HEINRICH, Industrial Accident Prevention, A Scientific Approach, Second edition, McGraw-Hill Book Company, New York and London, 1941.

[31.] HENDLEIN Teréz, PRAZSÁK Gergő: A hálózati társadalom receptje, Gondolatok Manuel Castells „A hálózati társadalom kialakulása" című könyvéről, 2005

[32.] HERODOTUS, „The Histories", London, England: J.M. Dent & Sons, Ltd, 1992

[33.] HORVÁTH Attila: A szellemi alkotások jogának története, a szerzői jogi védelem kialakulása, a jogalkotás kezdetei Magyarországon, Iparjogvédelmi és Szerzői Jogi Szemle, 11. (121.) évfolyam 4. szám, Budapest, 2016

[34.] HORVÁTH Gergely Krisztián, Kormányzati Informatikai Fejlesztési Ügynökség: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, Budapest, 2013.

[35.] Howard BILODEAU, Mohammad LARI, Mark UHRBACH, Cyber security and cybercrime challenges of Canadian businesses, The Canadian Centre for Justice Statistics, 2017

[36.] HSC (1993) Organising for Safety, 3rd Report of the Human Factors Study Group of the Advisory Committee on the Safety of Nuclear Installations, HSE Books

[37.] ILLÉSSY Miklós, NEMESLAKI András, SOM Zoltán: Elektronikus információbiztonság - tudatosság a magyar közigazgatásban, Információs Társadalom, Társadalomtudományi Folyóirat, 14 (1). pp. 52-73. ISSN 1587-8694, 2014

[38.] JAKAB Éva: Szerzők, kiadók, kalózok : a szellemi alkotások védelmének kialakulása Európában, Akadémiai Kiadó, Budapest, 2012.

[39.] James REASON, Human error: models and management, 2000.

[40.] James REASON, Managing the Risk of Organizational Accident, Routledge, 1997.

[41.] James REASON, Alan Hobbs: Managing Maintenance Error: A Practical Guide, 2003, James Reason's 12 Principles of Error Management

[42.] KAPLAN, NORTON, The Balanced Scorecard: Measures that Drive Performance, Harvard Business Review, 1992.

[43.] Kevin D. MITNICK, William L. SIMON: The art of deception, 2003

[44.] KESERŰ Barna Arnold, John Locke tulajdonelmélete a szellemi tulajdonjogok nézőpontjából, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar, 2016.

[45.] KIRÁLY Zoltán: A magyarországi számítástechnika története az első elektromos számítógép megjelenéséig, Budapest, 2009.

[46.] KISS Attila, KRASZNAY Csaba, A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai, Információs Társadalom, XVII. évf. (2017) 1. szám, Budapest, 2017.

[47.] KOVÁCS László, CZÉKMANN Zsolt, RITÓ Evelin, A mesterséges intelligencia alkalmazásának lehetőségei az államigazgatásban, Infokommunikáció és Jog, 2020/2. (75.), e-különszám

[48.] KOVÁCS László, KRASZNAY Csaba, Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság 2017/1. szám, 3–16.

[49.] KOVÁCSNÉ MOZSÁR Lívia Alice, Biztonságos informatikai alkalmazás portfólió menedzselés, Óbudai Egyetem, 2018.

[50.] KŐNIG Balázs, A közigazgatási információ-rendszerek fejlesztésének jogi környezete és vezetési intézményei, Informatikai rendszerek a közszolgálatban I., Scientia Rerum Politicarum, Sorozatszerkesztők: KISS György és KIS Norbert, Szerkesztette: SASVÁRI Péter, Dialóg Campus, Budapest, 2020.

[51.] KRASZNAY Csaba, Okoseszközök a kritikus információs infrastruktúrákban, Információ- és kiberbiztonság, Fenntartható biztonság és társadalmi környezet tanulmányok V., Sorozatszerkesztő: KIS Norbert, KOLTAY András, Szerkesztette: TÖRÖK Bernát, Budapest, 2020.

[52.] KRASZNAY Csaba, Kiberbiztonsági K+F+I Európában, Fenntartható biztonság és társadalmi környezet tanulmányok V., Sorozatszerkesztő: KIS Norbert, KOLTAY András, Szerkesztette: TÖRÖK Bernát, Budapest, 2020.

[53.] KRASZNAY Csaba, A közigazgatás IKT-infrastruktúrája és technológiaelemei, Informatikai rendszerek a közszolgálatban I., Scientia Rerum Politicarum, Sorozatszerkesztők: KISS György és KIS Norbert, Szerkesztette: SASVÁRI Péter, Dialóg Campus, Budapest, 2020.

[54.] Krisztina GYŐRFFY, Ferenc LEITOLD , Anthony ARROTT: Individual awareness of cyber-security vulnerability – Citizen and public servant, CEE eDem and eGov Days 2017: Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?, Budapest

[55.] Krisztina GYŐRFFYNÉ HOLLÓ: The Human Factors of the IT Risk Management, DUNAKAVICS, Dunaújvárosi Egyetem online folyóirata 2021. IX. évfolyam VII. szám, 47-61pp

[56.] Krisztina GYŐRFFYNÉ HOLLÓ, Adam KARISZTL: Domino effect and other models in the it process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

[57.] John LOCKE: Two Treatises of Government (Két értekezés a polgári kormányzatról), 1689

[58.] MÁDI-NÁTOR Anett, KARDOS Zoltán, , Információbiztonság-tudatosság gyakorlat, Nemzeti Közszolgálati Egyetem, https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsag-tudatossag-gyakorlat.original.pdf, letöltés: 2022. január 18.

[59.] MAGYARY Zoltán Közigazgatási-Fejlesztési Program (MP 12.0), Az elektronikus közigazgatás kiterjesztése, Budapest, 2012.

[60.] MAGYARY Zoltán, A Magyar Közigazgatás racionalizálása, Budapest, 1930.

[61.] MAGYARY Zoltán, A Magyar Közigazgatás gazdaságosságának és eredményességének biztosítása, A M. Kir. Miniszterelnök Úr elé terjesztett javaslat, Budapest, 1931.

[62.] Manuel CASTELLS: Az információ kora. Gazdaság, társadalom és kultúra, trilógia, A hálózati társadalom kialakulása, 1996., Az identitás hatalma, 1997., Az évezred vége, 1998.

[63.] Marvin RAUSAND, Risk Assessment Theory, Methods, and Applications, New Jersey, 2011.

[64.] MÁTHÉ Gábor, Intézménytörténet és jelenkor, Jogtörténeti szemle 3. sz., 1990. 103-105. oldal

[65.] MÁTHÉ Gábor, A hatalommegosztás kérdései, Jogtörténeti szemle 2. sz., 2004. 44-47. oldal

[66.] MOLNÁR Dóra: Kiberbiztonság Németországban – pillanatkép a német digitális térről, Nemzet és Biztonság 2018/1.

[67.] MUHA Lajos, Az informatikai biztonsági kockázatok elemzése, Robothadviselés, 2009

[68.] MUHA Lajos – SZÁDECZKY Tamás: Irányítási rendszerek, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[69.] MUHA Lajos (szerk.): Az informatikai biztonság kézikönyve, Verlag Dashöfer, Budapest, 2000-2005

[70.] MUHA Lajos: Az informatikai biztonság egy lehetséges rendszertana, [In.: Bolyai Szemle, XVII. évf. 4. szám, p. 137-156., Budapest: ZMNE BJKMK, ISSN: 1416-1443], Budapest, 2008.

[71.] MUHA Lajos: Informatikai biztonsági szabványok és irányelvek, GDF, Budapest, 2006

[72.] MUNK Sándor A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései, Haditechnika, 2018/1, Budapest, http://real.mtak.hu/77921/1/HT20181_115_133_u.pdf, Letöltés: 2018. június 10.

[73.] MUNK Sándor: A Magyar Honvédség informatikai interoperabilitási politikája, 2006. Ludita, a Nemzeti Közszolgálati Egyetem repozitórium-rendszere, letöltés: 2017. november 24.

[74.] M. ZAROUR, M. ALENEZI, A. K. SARKAR, A. AGRAWAL, R. KUMAR, R. A. KHAN, Healthcare Data Breaches: Insights and Implications, Healthcare 2020, 8(2), 133

[75.] NÁDASI András: Információtörténelem, Eger, 2011

[76.] NAGY Judit: Az ipar 4.0 fogalma, összetevői és hatása az értékláncra, Budapest, 2017

[77.] NEMESLAKI András, SASVÁRI Péter, Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában, Infokommunikáció és jog, 2014/4.(60.), 169-177.o.

[78.] NIVEN, Paul R.: Balanced scorecard step-by-step for government and nonprofit agencies, 32-33p, 2008.

[79.] NYIKES Zoltán: A biztonságtudatosság fejlesztésének egyes lehetőségei, Óbudai Egyetem, A XXII. Fiatal műszakiak tudományos ülésszak előadásai, Műszaki tudományos közlemények 7., Erdély, 2017

[80.] ÖTVÖS Gergő, Kiberbiztosítási trendek, Biztosítás és Kockázat, III. évfolyam 1. szám, 2016.

[81.] PART Krisztina Katalin: A szerzői jogi szabályozás kialakulása Angliában, Németországban és az Egyesült Államokban, Iparjogvédelmi és Szerzői Jogi Szemle, 1. (111.) évfolyam 4. szám, 2006.

[82.] PÉTERFALVI Attila, Átláthatóság a védelmi igazgatásban, Budapest, 2014.

[83.] PÉTERFALVI Attila, A magyar adatvédelmi jogi szabályozás változásai, in: Állam és Jog – Kodifikációs kihívások napjainkban, Magyar Jog- és Államtudományi Társaság – Gondolat, Szeged-Budapest, 2013

[84.] PÉTERFALVI Attila, ESZTERI Dániel, (2017) A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata. In: A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. ELTE Állam- és Jogtudományi Kar, Budapest, pp. 405-420., http://real.mtak.hu/97033/, letöltés: 2021. április 17.

[85.] Platón összes művei I., KERÉNYI Grácia fordítása, Európa, Budapest, 1984

[86.] Reece A. CLOTHIER, Brendan P. WILLIAMS, Neale L. FULTON, XunGuo LIN, ALARP and the Risk Management of Civil Unmanned Aircraft Systems, 2013

[87.] R. T. KAMURTHI, S. R. CHOPRA and R. SHARMA, Confrontation-Wi-Fi Risks and Data Breach, 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), 2021, pp. 633-638, doi: 10.1109/ESCI50559.2021.9397047.

[88.] Samuel JOHNSON (1709-1784), Angol szótár, 1755.

[89.] SHANNON, C. E., A Mathematical Theory of Communication, The Bell System Technical Journal, 1948.

[90.] SOM Zoltán, Kockázatmenedzsment gyakorlat, Nemzeti Közszolgálati Egyetem, 2014.

[91.] TARJÁN Gábor, Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben, Budapest, 2020.

[92.] TARPAI Zoltán, SZEÜSZ-ök – Koncepció és példák, Informatikai rendszerek a közszolgálatban II., Scientia Rerum Politicarum, Sorozatszerkesztők: KISS György és KIS Norbert, Szerkesztette: SASVÁRI Péter, Dialóg Campus, Budapest, 2020.

[93.] S. TRABELSI, Monitoring Leaked Confidential Data, 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2019, pp. 1-5

[94.] VARGA Zs. András, 4. Jogállamiság, Jogállamiság-paradigma a XIX. század elején, (CSINK Lóránt, SCHANDA Balázs, VARGA ZS. András, A magyar közjog alapintézményei, Budapest, Pázmány Press, 2020.)

[95.] VASSÁNYI István: Információelmélet jegyzet, Veszprémi Egyetem (Pannon Egyetem), Műszaki Informatika Kar, 2002-2012.

[96.] VREEKEN, A. (2005). "The History of Information: Lessons for Information Management," University of Amsterdam, Netherlands Sprouts: Working Papers on Information Systems, 5(2), fordította: NÁDASI András, Eger

[97.] Xue-Shan YAN: Information Science: Its Past, Present and Future, Department of Information Management, Peking University, Beijing 100871, China, 2011.

[98.] Warburton's Letter from an Author, London (1747), University of Birmingham Library: R. Hurd, ed., The Works of the Right Reverend William WARBURTON, 12 vols. (London: Cadell & Davies, 1811) Vol.12, 405-416

[99.] WAGNER, Paul, Third Party Breaches - A Survey of Threats and Recommendations, United States, 2021. SSRN http://dx.doi.org/10.2139/ssrn.3782822, letöltés: 2022. február 26.

[100.] WIENER, Norbert: Cybernetics or Control and Communication in the Animal and the Machine, 1948

[101.] WILHELM Gábor: Antropológiai tárgyelmélet, Pécs, 2010

[102.] Zachary FIGUEROA, Time to Rethink Cybersecurity Reform: The OPM Data Breach and the Case for Centralized Cybersecurity Infrastructure, 24 Catholic University Journal of Law and Technology, USA, (2016). https://scholarship.law.edu/jlt/vol24/iss2/7, letöltés: 2022. február 26.

[103.] Zöld könyv az infokommunikációs szektor 2014-2020 közötti fejlesztési irányairól, Budapest, 2014.

[104.] Z. YAZAR, A qualitative risk analysis and management tool – CRAMM, SANS InfoSec Reading Room White Paper, 2002 - Citeseer

Jogszabályok, rendelkezések, döntések és ajánlások

[1.] 15/1991. (IV. 13.) AB határozat

[2.] 138/2014. (IV. 30.) Korm. rendelet az árva mű felhasználásának részletes szabályairól

[3.] 1991. évi XXXVIII. törvény a használati minták oltalmáról

[4.] 1991. évi XXXIX. törvény a mikroelektronikai félvezető termékek topográfiájának oltalmáról

[5.] 1995. évi XXXIII. törvény a találmányok szabadalmi oltalmáról

[6.] 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról

[7.] 1997. évi XI. törvény a védjegyek és a földrajzi árujelzők oltalmáról

[8.] 1999. évi LXXVI. törvény a szerzői jogról

[9.] 2001. évi XLVIII. törvény a formatervezési minták oltalmáról

[10.] 2007. évi CI. törvény, a döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról

[11.] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[12.] 2012. évi C. tv. a Büntető törvénykönyvről

[13.] 2012. évi I. törvény a munka törvénykönyvéről

[14.] 2012. évi II. tv. a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről

[15.] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[16.] 2013/0027/COD, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148, 2022. március 6.

[17.] 2014. évi LXXVI. törvény a tudományos kutatásról, fejlesztésről és innovációról

[18.] 2016. évi XCIII. törvény a szerzői jogok és a szerzői joghoz kapcsolódó jogok közös kezeléséről

[19.] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

[20.] 29. cikk szerinti Adatvédelmi Munkacsoport a 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról szóló 06/2014. számú vélemény, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf, letöltés: 2021. december 23

[21.] 234/2011. (XI. 10.) Korm. rendelet, a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról, 2021. május 9-i állapot

[22.] 33/1998. (VI. 24.) NM rendelet a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről

[23.] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

[24.] ADATVÉDELMI BIZTOSOK NEMZETKÖZI KONFERENCIÁJA, A személyes adatok védelmének kompetencia keretrendszere diákok számára, Segédlet pedagógusok részére, 2016., https://www.naih.hu/files/kompetencia-keret-diakoknak.pdf, letöltés: 2022. január 16.

[25.] A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK Európai interoperabilitási keret – Végrehajtási stratégia, https://ec.europa.eu/transparency/regdoc/rep/1/2017/HU/COM-2017-134-F1-HU-MAIN-PART-1.PDF, Letöltés: 2018. június 13.

[26.] A DigComp 2.1 EU-ajánlás alapján kidolgozott javaslat a tanulók digitáliskompetencia-szintjeinek meghatározásához és fejlesztéséhez, Digitális Pedagógiai Fejlesztések Munkacsoport, Oktatási Hivatal, 2021.

[27.] A KIB 25. számú ajánlása: 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata, https://ugyintezes.magyarorszag.hu/dokumentumok/kib25ibiv.pdf, letöltés: 2018. június 7.

[28.] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet

[29.] A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2021. évi tevékenységéről, (B/18074) Nemzeti Adatvédelmi és Információszabadság Hatóság Budapest, 2022.

[30.] A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről, NAIH, 2016., https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf, letöltés: 2021. december 23

[31.] A TANÁCS 2005/222/IB KERETHATÁROZATA, (2005. február 24.), az információs rendszerek elleni támadásokról

[32.] Az Európai Bizottság szervezetirányítási rendszere: helyes gyakorlatok?, www.eca.europa.eu/lists/ecadocuments/sr16_27/sr_governance_hu.pdf, 2016. Luxembourg, letöltés: 2021. május 9.

[33.] Az európai digitális menetrend, http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=COM:2010:0245:FIN, letöltés: 2021. december 4.

[34.] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

[35.] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR) http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679, letöltés: 2017. december 20.

[36.] Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.), az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról, letöltés: 2019. november 24.

[37.] Az Európai Parlament és a Tanács 526/2013/EU rendelete, az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről, 2013

[38.] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály), letöltés: 2019. november 23.

[39.] Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről, http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32014R0910, letöltés: 2017. december 20.

[40.] Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről EGT-vonatkozású szöveg, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32012R1025, letöltés: 2019. november 24.

[41.] Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról (EGT-vonatkozású szöveg), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32015L1535 , letöltés: 2019. november 24.

[42.] Az Európai Parlament és a Tanács (EU) 2018/1725 Rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32018R1725&from=EN, letöltés: 2020. november 17.

[43.] A Tanács Határozata (2013. szeptember 23.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2013/488/EU), Brüsszel, 2013. https://eur-lex.europa.eu/legal-content/hu/TXT/PDF/?uri=CELEX:32013D0488&from=EN, letöltés: 2020. november 17.

[44.] Az Európai Unió Tanácsa, Approved cryptographic products – secret ue/eu secret, List of Approved Cryptographic Products (LACP)

[45.] BDSG, https://dsgvo-gesetz.de/bdsg/

[46.] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM(2009) 149., https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF, Letöltés: 2018. június 13.

[47.] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach, COM(2001) 298., https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52001DC0298, Letöltés: 2018. június 13.

[48.] Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" {SEC(2006) 656}, COM(2006) 251., https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52006DC0251, Letöltés: 2018. június 13.

[49.] Computer Emergency Response Team (CERT-EU) for the EU institutions, 2012. szeptember 11. után létrejött ügynökségek és szervek, https://cert.europa.eu/cert/plainedition/en/cert_about.html

[50.] Council of Europe (2018.), Reference Framework of Competences for Democratic Culture

[51.] COUNCIL OF THE EUROPEAN UNION, COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020, amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN, letöltés: 2022. február 26.

[52.] The Council of the European Union, Council Recommendation Of 22 May 2018 on key competences for lifelong learning, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0604(01)&rid=7, letöltés: 2021. december 18.

[53.] Die Digitale Agenda des BMI, Bundesministerium des Innern, Für Bau und Heima, Berlin, 2019., https://www.bmi.bund.de, letöltés: 2019. december 01.

[54.] Digital Education Action Plan (2021-2027), Resetting education and training for the digital age, https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en, 2021. május 2.

[55.] Digitális Magyarország, E-közigazgatási keretrendszer koncepció, Belügyminisztérium, 2015. április 29., Budapest

[56.] DS-GVO, https://e-justice.europa.eu/content_member_state_law-6-de-hu.do?member=1

[57.] Egyezmény az emberi jogok és alapvető szabadságok védelméről, Róma, 1950. november 4.

[58.] ENISA, Addressing Skills Shortage and Gap Through Higher Education, riport, 2021.

[59.] Európai Digitális Kompetencia Keretrendszer, European Digital Competence Framework, DigComp 2.1, https://ec.europa.eu/jrc/en/digcomp, 2017.

[60.] Európai Hálózat- és Információbiztonsági Ügynökség (ENISA), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Al24153, letöltés: 2022. augusztus 7.

[61.] Európai Bizottság: Európai interoperabilitási keret – Végrehajtási stratégia (2017), https://ec.europa.eu/transparency/regdoc/rep/1/2017/HU/COM-2017-134-F1-HU-MAIN-PART-1.PDF, letöltés: 2021. december 10.

[62.] Európai Munkahelyi Biztonság és Egészségvédelmi Ügynökség: Framework Agreement on Telework

[63.] Európai Unió: A Tanács Határozata (2013. szeptember 23.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2013/488/EU), Brüsszel, 2013. https://eur-lex.europa.eu/legal-content/hu/TXT/PDF/?uri=CELEX:32013D0488&from=EN letöltés: 2020. november 17

[64.] Európai uniós irányelvek, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Al14527, Letöltés: 2018. június 11.

[65.] European Data Protection Board, Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021, Version 1.0, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf letöltés: 2022. január 15.

[66.] European Data Protection Board, Guidelines 01/2021 on Examples regarding Data Breach Notification, Version 2.0, https://edpb.europa.eu/our-work-

tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en, letöltés: 2022. január 15.

[67.] European Framework for the Digital Competence of Educators, DigCompEdu, https://ec.europa.eu/jrc/en/digcompedu, 2017.

[68.] European Cybersecurity Month 2020 - Deployment Report, ENISA, https://www.enisa.europa.eu/publications/ecsm-deployment-report-2020, letöltés: 2021. április 24.

[69.] European Union Agency for Network and Information Security, (ENISA), Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, 2018. december

[70.] Gazdasági Együttműködési és Fejlesztési Szervezet, Az információs rendszerek és hálózatok biztonságára vonatkozó OECD irányelvek: Útban a biztonságkultúra felé, 1992. https://www.oecd.org/sti/ieconomy/15582292.pdf Áttekintés, 2003.

[71.] Gesetz zur Förderung des elektronischen identitätsnachweises, 2017., https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2310.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2310.pdf%27%5D__1575469181569, letöltés: 2019. december 4.

[72.] HDSIG, https://datenschutz.hessen.de/infothek/gesetze

[73.] ISO 31000, Terms and definitions

[74.] Information Security Management System, ISO/IEC 27000:2013, szabványcsalád

[75.] Information Security Management System, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001 szabvány - Információbiztonsági Irányítási Rendszer, https://www.iso.org/isoiec-27001-information-security.html, letöltés: 2021. április 24.

[76.] ISO Guide 73, Risk management, Vocabulary

[77.] Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE, a hálózat- és információbiztonságának az egész Unióban egységesen magas szintre vonatkozó intézkedésekről, COM/2013/048 final – 2013/0027 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013PC0048, Letöltés: 2018. június 13.

[78.] Közigazgatási Informatikai Bizottság, Magyar Informatikai Biztonsági Keretrendszer (MIBIK - KIB 25. sz. ajánlása 1.), Informatikai Biztonsági Irányítási Rendszer (IBIR - KIB 25. sz. ajánlása 1-1.), az Informatikai Biztonság Irányítási Követelmények (IBIK -

KIB 25. sz. ajánlása 1-2.), Informatikai Biztonság Irányításának Vizsgálata (IBIV - KIB 25. sz. ajánlása 1-3.)

[79.] Leitfaden zum Digitalisierungsprogramm des IT-Planungsrates, 2019., https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Digitalisierungsprogramm/DigPro_Leitfaden.html?nn=11113802, letöltés: 2019. december 4.

[80.] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat

[81.] MSZ ISO/IEC 27001:2014 szabvány, Erőforrások kezelése

[82.] National Audit Office, Investigation: WannaCry cyber attack and the NHS, by the Comptroller and Auditor General, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf, letöltés: 2021. április 3.

[83.] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), A Nemzeti Adatvédelmi és Információszabadság Hatóság 2020. évi beszámolója, VII. Nemzetközi ügyek és társadalmi kapcsolatok,164.o., https://www.naih.hu/eves-beszamolok, letöltés: 2021. április 3.

[84.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Adatvédelmi szótár, https://naih.hu/adatvedelmi-szotar, letöltés: 2021. március 20.

[85.] Nemzeti Adatvédelmi és Információszabadság Hatóság, A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), közleménye az Erzsébet-táborokban a táborozó gyermekek részére készített, „Véleményed kincs!” című kérdőívhez kapcsolódó adatkezelést illetően, 2020.

[86.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Online Ügyindítás - e-Papír

[87.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Tájékoztatók, ajánlások, Interneten elkövetett bűncselekményekre hívja fel a figyelmet a linken elérhető videó, https://www.naih.hu/tajekoztatok-ajanlasok, Say No! (Hungarian) - A campaign against online sexual coercion and extortion of children, https://www.youtube.com/watch?v=ufTgIJ2zKTE letöltés: 2022. január 15.

[88.] Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH-1938-2/2013/T, Gyakorlati útmutató védett adatot nem tartalmazó kivonat készítéséhez, 2014., https://naih.hu/files/2014_02_03_anonimizalas_gyak_utm.pdf, letöltés: 2022. január 14.

[89.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: Határozat hivatalból indult hatósági eljárásban, Ügyszám: NAIH/2020/2729/15

[90.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: Határozat hivatalból indult hatósági eljárásban, Ügyszám: NAIH/2020/2758/4.

[91.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban Ügyszám: NAIH/2019/2471/6

[92.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban Ügyszám: NAIH/2020/66/21

[93.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: kérelemnek részben helyt adó határozat, Ügyszám: NAIH/2020/876/12. (NAIH/2019/8236.)

[94.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: kérelemnek helyt adó határozat, Ügyszám: NAIH/2020/4762/9.

[95.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Határozat, Tárgy: kérelemnek részben helyt adó határozat, hivatalbóli eljárást megszüntető határozat, jogsértés megállapítása Iktatószám: NAIH/2020/5553, korábbi ügyszám: NAIH/2019/346

[96.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Ügyszám: NAIH/2020/7127/ Tájékoztató a digitális távoktatás adatvédelmi és adatbiztonsági vonatkozásairól, III.5

[97.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Ügyszám: NAIH-3706-2/2021, Állásfoglalás a digitális távoktatás keretében a tankerületi igazgató, mint munkáltató és a pedagógus, mint foglalkoztatott között megköthető, a munkáltató által a munkavégzéshez biztosított, valamint a saját információtechnológiai vagy számítástechnikai eszközök, rendszerek használatáról szóló megállapodás adatvédelmi és adatbiztonsági vonatkozásairól, II.

[98.] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Kulcs a Net világához! A NAIH tanulmánya a gyermekek biztonságos és jogtudatos internethasználatáról https://www.naih.hu/files/2013-projektfuzet-internet.pdf, 23-24.o., 2013., letöltés: 2021. április 27.

[99.] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Kulcsocska a net világához, https://naih.hu/files/kulcsocska-a-net-vilagahoz-2018-01-29.pdf, 2017.

[100.] Nemzeti Adatvédelmi és Információszabadság Hatóság, Szemelvények az információs jogok felügyeletének elmúlt 25 évéből, szerk: Dr. Péterfalvi Attila

[101.] Nemzeti Közszolgálati Egyetem, Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-

tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok, letöltés: 2021. április 14.

[102.] Oktatási Hivatal, NAT, Digitális kultúra tantárgy, 2020.

[103.] Római Szerződés (EGK), Az Európai Gazdasági Közösséget (EGK-t) létrehozó szerződés, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Axy0023, letöltés: 2018. június 7.

[104.] Shaping Europe's digital future, Proposal for directive on measures for high common level of cybersecurity across the Union, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union, letöltés: 2021. április 24

[105.] Seveso-irányelv, Veszélyes anyagokkal kapcsolatos súlyos balesetek, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l21215&from=HU, 1976-ban történt seveso-i katasztrófa következtében a balesetek megelőzésére és kezelésére vonatkozó jogszabály

[106.] Szellemi Tulajdon Nemzeti Hivatala, https://www.sztnh.gov.hu/hu/mit-jelent/mit-jelent-a-szellemi-tulajdon, letöltés: 2019. június 1.

[107.] Szellemi Tulajdon Nemzeti Hivatala, https://www.sztnh.gov.hu/hu/szellemi-alkotas, letöltés: 2018. január 30.

[108.] The 2018 PREDICT Key Facts Report, JRC Technical report (by the Joint Research Centre), 2018., https://publications.jrc.ec.europa.eu/repository/bitstream/JRC112019/jrc112019_2018_predict_key_facts_report.pdf, letöltés: 2019. december 3.

[109.] Umsetzung des Onlinezugangsgesetzes (OZG), Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG), 2017. http://www.gesetze-im-internet.de/ozg/, hatályba lépés: 2017. nyara, letöltés: 2019. december 4.

[110.] Uniós adatvédelmi szabályok, dokumentumtár, Vegye át az irányítást GDPR virtuális személyazonossága fölött!, 2019., https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_hu#az-ltalnos-adatvdelmi-rendelet-pozitv-eredmnyek, letöltés: 2021. április 21.

[111.] Zielbild des Digitalisierungsprogramms, Quelle: Bundesministerium des Innern, für Bau und Heimat, 2019., letöltés: 2019. december 4.

Egyéb hivatkozások

[1.] 2011 State of Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey America's K–12 schools not preparing kids for digital age, study finds, https://www.prnewswire.com/news-releases/2011-state-of-cyberethics-cybersafety-and-cybersecurity-curriculum-in-the-us-survey-121240319.html, 2021. január 20.

[2.] AG Shapiro Announces Multistate Settlement With American Medical Collection Agency Over 2019 Data Breach, Pennsylvania Office of Attorney General, 2021., letöltés: 2022. február 26.

[3.] Avinor Oslo Airport: A new border control solution by IDEMIA, International Airtorp review, 2019., Avinor rolls out end-to-end touchless travel programme, International Airtorp review, 2020.

[4.] Bankkártya adatokat szivárogtatott egy kanadai mobil szolgáltató, Nemzeti Kibervédelmi Intézet, 2019. https://nki.gov.hu/it-biztonsag/hirek/bankkartya-adatokat-szivarogtatott-egy-kanadai-mobil-szolgaltato/, letöltés: 2022. február 26.

[5.] Australian National University, ANU releases detailed account of data breach (2019.)

[6.] California Department of Insurance, Anthem Data Breach, (2015)

[7.] C-311/18. sz. ügy, Data Protection Commissioner kontra Facebook Ireland Limited, Maximillian Schrems

[8.] Cyber Security Agency of Singapore, Singapore Cyber Landscape 2018.

[9.] Cyber security and cybercrime challenges of Canadian businesses, 2017, https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.htm, letöltés: 2020. Október 30.

[10.] Cybersecurity Workforce Study, 2020. https://www.isc2.org/Research/Workforce-Study, letöltés: 2021. december 18.

[11.] COSO Enterprise Risk Management – Integrated Framework, https://www.coso.org/pages/erm-integratedframework.aspx, letöltés: 2021. május 9.

[12.] Bundesministerium Für Wirtschaft Und Klimaschutz, Das Internet Governance Forum, https://www.bmwi.de/Redaktion/DE/Videos/2019/20191129-igf-2019-tag4.html, letöltés: 2019. december 6.

[13.] Das waren die Roots: Wie das Internet nach Deutschland kam, https://www.heise.de/newsticker/meldung/Das-waren-die-Roots-Wie-das-Internet-nach-Deutschland-kam-120535.html, letöltés: 2019. december 3.

[14.] ELTE Jogi Továbbképző Intézet, Adatbiztonsági és adatvédelmi jogi szakokleveles szakember képzés, https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-jogi-szakokleveles-szakember.t.562, letöltés: 2022. július 29.

[15.] ELTE Jogi Továbbképző Intézet, Adatbiztonsági és adatvédelmi szakjogász, https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406, letöltés: 2022. augusztus 2.

[16.] ENISA Threat Landscape 2015.

[17.] ENISA Threat Landscape 2020 - Data Breach, October 20, 2020

[18.] ENISA Threat Landscape 2021

[19.] ESET, A kiberbűnözők fertőzött weboldalakat használnak a kriptovaluták bányászatára ESET, hírek, https://www.eset.com/hu/rolunk/hirek/sajtokoezlemenyek/hogyan-lehetsz-tudtodon-kivul-kriptobanyasz/, letöltés: 2022. február 26.

[20.] ESET, Az erőforrásaink megszerzése miatt feltört gépek után, most hamis kriptovaluta tőzsdei alkalmazás tűnt fel a Google Play áruházban, ESET, hírek, https://www.eset.com/hu/hirek/kriptovaluta-elleni-bunozes/, letöltés: 2022. február 26.

[21.] European Council, EU imposes the first ever sanctions against cyber-attacks (2020.)

[22.] Európai Unió Tanácsa és az Európai Tanács, Rosszindulatú kibertámadások: uniós szankciók a Bundestag elleni 2015-ös kibertámadásért felelős két személlyel és egy szervvel szemben (2020.)

[23.] Eurostat: Employed persons working from home as a percentage of the total employment, by sex, age and professional status (%) https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=lfsa_ehomp&lang=en letöltés: 2020. november 18.

[24.] EUROPOL, Online sexual coercion and extortion is a crime, https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime, letöltés: 2022. január 15.

[25.] EUROPOL, Internet Organised Crime Threat Assessment (IOCTA) 2021, https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021, letöltés: 2022. január 15.

[26.] FBI, Advanced Fingerprint Identification Technology (AFIT), https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi, letöltés: 2021. május 5.

[27.] FBI, NGI, https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view, letöltés: 2021. május 5.

[28.] Felsőoktatási képzések, Óbudai Egyetem, Neumann János Informatikai Kar, https://nik.uni-obuda.hu/kepzesek/, Neumann János Egyetem, GAMF Műszaki és Informatikai Kar, https://gamf.uni-neumann.hu/kepzeseink/, Miskolci Egyetem, Gépészmérnöki és Informatikai Kar, https://www.iit.uni-miskolc.hu/oktatas.html Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar, https://www.vik.bme.hu/oktatas/, Pannon Egyetem, Műszaki Informatikai Kar, https://mik.uni-pannon.hu/index.php/hu/felveteli-menu/felveteli-a-mik-en.html, letöltés: 2022. január 18.

[29.] Health and Safety Executive, https://www.hse.gov.uk/managing/theory/index.htm, letöltés: 2021. május 9.

[30.] Health and safety guidance (HSG), Reducing error and influencing behaviour, United Kingdom for The Stationery Office (TSO), second edition 1999.

[31.] IBM, Ponemon Institute, Cost of Data Breach Study, 2017

[32.] Information Assurance, Situation In Switzerland And Internationally, Federal IT Steering Unit FITSU, Federal Intelligence Service FIS, Reporting and Analysis Centre for Information Assurance MELANI, 2016.

[33.] International Conference of Data Protection and Privacy Commissioners, RESOLUTION TO ADDRESS THE ROLE OF HUMAN ERROR IN PERSONAL DATA BREACHES, 41. International Conference of Data Protection and Privacy Commissioners, Tirana, Albania, sponsor: Office of the Australian Information Commissioner, Australia, 2019.

[34.] International Organization for Standardization, https://www.iso.org/about-us.html , letöltés: 2022. március 6.

[35.] International cyber law, The Shadow Brokers publishing the NSA vulnerabilities (2016)

[36.] Kiberfenyegetések és kibervédelem, Országgyűlés Hivatala, Infojegyzet, 2016/44., Budapest, 2016. szeptember 29.

[37.] Magyar Szabványügyi Testület, http://www.mszt.hu/web/guest/a-szabvanyositas-tortenete, letöltés: 2021. november 23.

[38.] Milliárdokat költenek védelemre, mégis simán kijátsszák őket!, http://www.biztositasiszemle.hu/cikk/nemzetkozihirek/eu/milliardokat_koltenek_vedelemre_megis_siman_kijatsszak_oket.6582.html, letöltés: 2022. február 26..

[39.] NASA, Risk Management Reporting, 2009.

[40.] Nem kémkednek tovább az LG okostévéi, 2013. november 22., https://pcworld.hu/eletmod/nem-kemkednek-tovabb-az-lg-okostevei-141629.html, letöltés: 2017. december 10.

[41.] Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/tananyagok

[42.] Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, Elektronikus információbiztonsági vezető szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/tananyagok

[43.] Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, Digitális térségfejlesztés szakirányú továbbképzési szak, Integritás tanácsadó szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/altalanos-informaciok, Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak, https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok, letöltés: 2022. január 17.

[44.] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, IT biztonság, Hírek, Több, mint 50 000 otthoni IP kamerát tört fel egy hacker csoport, https://nki.gov.hu/it-biztonsag/hirek/tobb-mint-50-000-otthoni-kamerat-tort-fel-egy-hacker-csoport/, 2020. október 21., letöltés: 2022. augusztus 7.

[45.] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, IT-biztonsági sajtószemle, https://nki.gov.hu/it-biztonsag/kiadvanyok/sajtoszemle/, Időszak: 201-2021. letöltés: 2022. augusztus 7.

[46.] Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, IT-biztonsági tanácsok, https://nki.gov.hu/it-biztonsag/tanacsok/, letöltés: 2022. augusztus 7.

[47.] NRC Marketingkutató és Tanácsadó Kft., Nőtt az internetpenetráció, már 6 175 500 fő internetezik hazánkban, https://nrc.hu/news/internetpenetracio-2/, letöltés: 2021. április 27.

[48.] OECD Guidelines for the Security of Information Systems, 1992

[49.] Országgyűlés Hivatala: Infojegyzet 2020/7 https://www.parlament.hu/documents/10181/4464848/Infojegyzet_2020_7_tavmunka.pdf/80c2a726-b98d-0c81-363e-1f1023acab8e?t=1585506935186, letöltés: 2020. november 18.

[50.] Possible Phishing Campaigns Arising from Facebook's Data Leak, Government of Singapore, 2021.

[51.] Sans Institute, CIS Critical Security Controls, https://www.sans.org

[52.] Sans Institute, Data Breach Report, (DBR) 2020. https://www.sans.org/blog/2020-data-breach-incident-report-dbir/, letöltés: 2021. március 30.

[53.] Singapore Government Agency: Singapore International Cyber Week 2020, https://www.csa.gov.sg/news/press-releases/sicw-2020-highlights-and-testimonials, letöltés: 2020. október 30.

[54.] Sok veszélyt tartogat a jövő év a vállalkozások számára, http://www.biztositasiszemle.hu/cikk/elemzesek/NULL/sok_veszelyt_tartogat_a_jovo_ev_a_vallalkozasok_szamara.6201.html, letöltés: 2021. december 10.

[55.] Spanish DPA Fines Vodafone Spain more than 8 Million Euros, https://edpb.europa.eu/news/national-news/2021/spanish-dpa-fines-vodafone-spain-more-8-million-euros_hu, letöltés: 2021. április 24.

[56.] Statista Research Department: Impact of cyber security incidents in Singapore 2016 https://www.statista.com/statistics/787025/singapore-impact-of-cyber-security-incidents-on-firms/, letöltés: 2020. október 30.

[57.] Jon DIMAGGIO, The Black Vine cyberespionage group, Symantec, 2015.

[58.] Transportation Security Administration (TSA), https://www.epic.org/apa/comments/EPIC-TSA-Pre-Check-Expansion-Comments.pdf, letöltés: 2021. május 5.

[59.] Verizon Data Breach Incident Report 2020

[60.] Varonis: The World in Data Breaches (Breach Level Index) https://www.varonis.com/blog/the-world-in-data-breaches/, letöltés: 2020.november 15.

[61.] The World Wide Web Security FAQ, W3, https://www.w3.org/Security/Faq/wwwsf6.html, letöltés: 2022. február 26.

[62.] Wolters Kluwer – Hungary, https://net.jogtar.hu/, statisztikai adatok összegyűjtése: 2021. március 20

HOLLÓ KRISZTINA PUBLIKÁCIÓS JEGYZÉKE

[1.] Eszter OROSZI , Krisztina GYŐRFFY: Information security for egovernment social media marketing and citizen interaction, Central and Eastern European eIDem and eIGov Days 2016: Multi-Level (e)Governance: Is ICT a means to enhance transparency and democracy?, Budapest, 2016.

[2.] Ferenc, LEITOLD, Kálmán HADARICS , Eszter OROSZI , Krisztina GYŐRFFY: Measuring the information security risk in an infrastructure, MALWARE 2015 10th International Conference on Malicious and Unwanted Software, Puerto Rico, 2015

[3.] Ferenc LEITOLD, Krisztina GYŐRFFYNÉ HOLLÓ, Zoltán KIRÁLY, Quantitative metrics characterizing malicious samples, In: Cyril, Onwubiko; Pierangelo, Rosati; Aunshul, Rege; Arnau, Erola; Xavier, Bellekens; Hanan, Hindy; Martin Gilje, Jaatun (szerk.) Cyber Science, CyberSA for Trustworthy and Transparent Artificial Intelligence (AI), Dublin, Írország: Center for Multidisciplinary Research, Innovation and Collaboration 2021. pp. 82-83., 2 p.

[4.] GYŐRFFYNÉ HOLLÓ Krisztina: Az információbiztonság jelentősége és története, GRADUS Vol 8, No 2 (2021), John von Neumann University, Hungary, Kecskemét

[5.] GYŐRFFYNÉ HOLLÓ Krisztina, Információbiztonság, avagy incidens kontra biztonságtudatos viselkedés, INFOKOMMUNIKÁCIÓ ÉS JOG 18., 76 pp. 17-23. 7 p., 2021.

[6.] GYŐRFFYNÉ HOLLÓ Krisztina, Az érintés nélküli adatgyűjtés kockázatai és a kockázatszámítás módszerei, DUNAKAVICS 9 : 8 pp. 77-97. , 21 p., 2021.

[7.] GYŐRFFYNÉ HOLLÓ Krisztina, Közszolgálati információs rendszerek interoperabilitási nehézségeinek megoldása, DUNAKAVICS 2021. IX. évfolyam II. szám pp. 21-40. , 19 p., 2021.

[8.] GYŐRFFYNÉ HOLLÓ Krisztina, LEITOLD Ferenc: Felhasználókkal kapcsolatos információbiztonsági intézkedések kezelése a GDPR tükrében, Hétpecsétes történetek 2,5 - a GDPR antológia, Budapest, 2018.

[9.] GYŐRFFYNÉ HOLLÓ Krisztina, Az információbiztonsági sebezhetőségek tényezőinek vizsgálata: A „humán faktor”, In: Váraljai, Mariann (szerk.) INFORMATIKA KORSZERŰ TECHNIKÁI KONFERENCIA 2021 „Jövőformáló tudomány” „Fenntarthatóság és digitalizáció” Dunaújváros 2021. november 9.: DUE Press (2021) 80 p. p. 40

[10.] GYŐRFFYNÉ HOLLÓ Krisztina, Információbiztonság, avagy megéri kockáztatni? In: Nagy, Bálint; Katona, József AZ INFORMATIKA KORSZERŰ TECHNIKÁI KONFERENCIA 2020 : Jövőformáló tudomány programfüzet és absztraktkötet Dunaújváros, 2020. november 9-10., Dunaújváros, DUE Press 2020. 48 p.p. 22

[11.] GYŐRFFYNÉ HOLLÓ Krisztina, Az információbiztonsági tudatos viselkedés az incidensek elkerülésének egyik tényezője, DUNAKAVICS 8 : 12 pp. 5-18. , 14 p. 2020.

[12.] HADARICS, K., GYORFFY, K., Nagy, B., BOGNAR, L., ARROTT, A., LEITOLD, F., Mathematical Model of Distributed Vulnerability Assessement, Security and Protection of Information 2017, University of Defence, IDET BRNO, Czech Republic, 2017

[13.] Krisztina GYŐRFFY, Ferenc LEITOLD , Anthony ARROTT: Individual awareness of cyber-security vulnerability – Citizen and public servant, CEE eDem and eGov Days 2017: Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?, Budapest

[14.] Krisztina GYŐRFFYNÉ HOLLÓ: The Human Factors of the IT Risk Management, DUNAKAVICS, Dunaújvárosi Egyetem online folyóirata 2021. IX. évfolyam VII. szám, 47-61pp

[15.] Krisztina GYŐRFFYNÉ HOLLÓ, Adam KARISZTL: Domino effect and other models in the it process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

ÁBRAJEGYZÉK

RÖVIDÍTÉSEK JEGYZÉKE

AEPD: Agencia Española de Protección de Datos, Spanyol Adatvédelmi Hatóság

Akr: 2016. évi CL. törvény, az általános közigazgatási rendtartásról

Avtv: 1992. évi LXIII. törvény, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

BCP: Business Continuity Planning

BDSG: Bundesdatenschutzgesetz

BEA: Bureau of Enquiry and Analysis, model (French, Loss of control accident model)

BMI: Bundesministerium des Innern

BSI: British Standards Institution

BSI: Bundesamt für Sicherheit in der Informationstechnik

CCNA: Cisco Certified Network Associate

CEH: Certified Ethical Hacker

CERT: Computer Emergency Response Team

CFSP: Common Foreign And Security Policy (Council Of The European Union, Council Decision)

CFT: Contactless Fingerprint Technologies

CIS: Critical Security Controls

CISM: Certified Information Security Manager

CISSP: Certified Information Systems Security Professional

CJIS: Criminal Justice Information Services (FBI)

COBIT: Control Objecitves for Information and Related Technology

COSO: Committee of Sponsoring Organizations

COVID-19 (SARS-CoV-2): coronavirus disease - koronavírus okozta megbetegedés, Severe Acute Respiratory Syndrome - súlyos heveny légúti tünetegyüttes vírusa, 2019.

CRAMM: CCTA Risk Analysis and Management Method

CSA: Cyber Security Agency of Singapore, Szingapúri Kiberbiztonsági Ügynökség

CSA: EU kiberbiztonsági rendelete

CSIRT: Computer Security Incident Response Team

CTI: Cyber threat intelligence

CySA+: Cybersecurity Analyst

CyberHEAD: Cybersecurity Higher Education Database

DBIR: Data Breach Incident Report

DBR: Data Breach Report

DDoS: Distributed Denial of Service

DPA: Dutch Data Protection Authority, Holland Adatvédelmi Hatóság

DPO: data protection officer, adatvédelmi tisztviselő

DS-GVO: Datenschutz-Grundverordnung

DSAnpUG-EU: Datenschutz-Anpassungs- und Umsetzungsgesetz EU

DTI/CCSC: Department of Trade and Industry's, Commercial Computer Security Centre (Kereskedelmi és Ipari Minisztérium, Kerekedelmi Számítógép Biztonsági Központ)

DigComp: European Digital Competence Framework, Európai Digitális Kompetencia Keretrendszer

DigCompEdu: European Framework for the Digital Competence of Educators

EBESZ: Európai Biztonsági és Együttműködési Szervezet, Organization for Security and Co-operation in Europe, OSCE

ECSM: European Cybersecurity Month, Európai Kiberbiztonsági Hónap

EDPB: European Data Protection Board, Európai Adatvédelmi Testület

EGK: Európai Gazdasági Közösség

EIF: Európai Interoperabilitási Keretrendszer

EJEE: emberi jogok európai egyezménye

ENISA: European Union Agency for Cybersecurity (European Union Agency for Network and Information Security), Európai Uniós Kiberbiztonsági Ügynökség

ENSZ: Egyesült Nemzetek Szervezete, United Nations, alapítva: Alapítva: 1945. San Francisco, Székhely: New York

EPIC: Electronic Privacy Information Center, Elektronikus Adatvédelmi Információs Központ

ERM: Enterprise Risk Management

ETA: Event-tree Analysis

ETL: ENISA Threat Landscape

EU: Európai Unió

FMCEA: Failure Mode, Effects and Criticality Analysis

FMEA: Failure Mode and Effects Analysis

FTA: Fault Tree Analysis

GDPR: General Data Protection Regulation

HACCP: Hazard Analysis and Critical Control Points

HAZOP: Hazard and Operability Studies

HDSIG: Gesetzestext Hessisches Datenschutz- und Informationsfreiheitsgesetz

HSE: Health, Safety and Environment

IB: információbiztonság

IBtv: 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

IEC (International Electrotechnical Commission): Nemzetközi Elektrotechnikai Bizottság, alapítva: 1906. London, nemzetközi szabványügyi szervezet, székhelye: Genf

IGF: Internet Governance Forum

IKT (ICT): információs és kommunikációs technológiák

IMI: Internal Market Information System, Belső Piaci Információs Rendszer

IP: Internet Protocol

ISACA: Information System Audit Control Association

ISMS: Information Security Management System

ISO: International Organisation of Standards

IT: Information Technology

ITIL: Information Technology Infrastructure Library

ITU: Nemzetközi Távközlési Egyesület

Infotv: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

KRESZ: Közúti Rendelkezések Egységes Szabályozása, 1/1975. (II. 5.) KPM-BM együttes rendelet a közúti közlekedés szabályairól

LDAP: Lightweight Directory Access Protocol

MAC: Media Access Control

MDM: Mobile Devices Management

MFA: Multi-factor authentication

MI (AI): mesterséges intelligencia

MP: Magyary Program

MSZ: Magyar Szabványügyi Testület, Forrásszabvány nélküli – úgynevezett tiszta MSZ – szabványok kidolgozása, Európai/nemzetközi szabványok magyar nyelvű bevezetése

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság

NATO: North Atlantic Treaty Organisation, Észak-atlanti Szerződés Szervezete, alapítva: 1949. Washington, Székhely: Brüsszel

NBSZ NKI: Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet

NCSC: Egyesült Királyság Nemzeti Kiberbiztonsági Központja

NGI: Next Generation Identification

NISD: Network and Information Security Directive

NIST: National Institute of Standards and Technology

NSA: National Security Agency, USA

OECD: Organisation for Economic Co-operation and Development, Gazdasági Együttműködési és Fejlesztési Szervezet, Párizs

OPCW: Organisation for the Prohibition of Chemical Weapons

OWASP: Open Web Application Security Project

OZG: Umsetzung des Onlinezugangsgesetzes

PDCA: Pland Do Check Act

PIAAC: Programme for the International Assessment of Adult Competencies

RISC: Repository for Individuals of Special Concern (FBI)

SGB: Sozialgesetzbuch

SQL: Structured Query Language

TKG: Telekommunikationsgesetz

TMG: Telemediengesetz

TSA: Transportation Security Administration, USA

TÜV: TÜV Rheinland vizsgálati jele

VPN: virtual private network

TÁBLÁZATOK JEGYZÉKE

1. SZÁMÚ MELLÉKLET, A BALANCED SCORECARD MÓDSZER

A módszert Robert S. Kaplan és David P. Norton dolgozta ki a 90-es években, amely „kiegyensúlyozott stratégiai mutatószámrendszer”-ként vált ismerté. 1990-ben Kaplan és Norton számos cég kutatási tanulmányát vezette, és egyben új, hatékonyabb mérési módszereket kutattak. A tanulmányozó vállalatok, így Kaplan és Norton meg volt győződve arról, hogy a teljesítmény pénzügyi mércéire való támaszkodás befolyásolja a szervezet értékteremtő képességét. A kutatócsoport megvitatta a lehetséges alternatívákat, meghatározta az eredménymutató módszerét, amelyek többek között a szervezet egészét lefedő teljesítménymérési lépéseit tartalmazta, úgymint az ügyfelek vagy érdekelt felek kérdéseit, a belső üzleti folyamatokat, a munkavállalói tevékenységeket és tudatosítást és persze a befektetői kérdéseket.[465] A módszer sikerességén túl az eredménymutatóhoz kiválasztott intézkedések olyan eszközként szolgálnak a vezetők és a szervezetek számára, amelyek révén a szervezet valószínű el fogja érni küldetését és stratégiai céljait.[466] A modell tulajdonképpen a szervezeti stratégiához kapcsolódó, megfelelően megválasztott és részletesen kidolgozott felmérések folyamata. Olyan eszközt biztosít a szervezet vezetői számára, amely egy könnyen átlátható megnyilvánulási forma – úgynevezett stratégiai térkép – segítségével mind a munkatársak, mind a külső érdekeltek irányába kommunikálható a szervezet stratégiája, és az elérni kívánt eredmény. Lényegében a Balanced Scorecard nemcsak egy kommunikációs eszköz, hanem egy komplex mérési és stratégiai menedzsment rendszer[467], amelynek összefoglaló felülete a stratégiai térkép. A Balanced Scorecard módszer a kutatási projekt információbiztonsági „termékének” bemutatásához használható. A Balanced Scorecard modell kívül matematikai, információbiztonsági módszereket is alkalmaztam, amelyek háttérkutatás módszereként szerepeltek az adatvédelmi és információbiztonsági kutatásom során.

[465] Kaplan, Norton, The Balanced Scorecard: Measures that Drive Performance, Harvard Business Review, 1992.

[466] Paul R. Niven: Balanced scorecard step-by-step for government and nonprofit agencies, 32-33p, 2008.

[467] Paul R. Niven: Balanced scorecard step-by-step for government and nonprofit agencies, 13p, 2008.

2. SZÁMÚ MELLÉKLET, A SZELLEMI ALKOTÁSOK JOGTÖRTÉNETE ÉS VÉDELME

Jogtörténeti szempontból a szellemi tulajdon és a szellemi alkotások felismerése és szabályozásának igénye időben az ideák és az információ filozófiai, valamint az információelmélet és az információbiztonság tudományos és jogi megfogalmazása közé tehető, ezért ebben a témakörben a szellemi tulajdon jogtörténeti vizsgálata jelentős. Az információ, amennyiben az beépül egy új szellemi alkotásba, és ahogy a szellemi alkotás egészére vonatkozik a szerzői jog védelme, úgy ebben az esetben az adott információra is. A szellemi tulajdon alatt az alkotó által megteremtett elméleti termék értendő. E témakörbe tartozik a találmány, az irodalmi és művészeti alkotás, valamint a kereskedelemben alkalmazott megjelölés, név, kép illetve forma. A szellemi tulajdon tárgyai jogi védelem alá tartoznak, ami biztosítja, hogy a találmányok vagy egyéb alkotások jogosultjai tevékenységükért megfelelő erkölcsi és anyagi elismerésben részesüljenek.[468] A védelmi eljáráshoz hozzátartozik az a tény, hogy pusztán egy ötlet nem oltalmazható. Az ötlet kidolgozása és annak megvalósítása esetén, így kutatásból származó eredmény, találmány kidolgozása, novella megírása, logó megalkotása is alkalmas lehet arra, hogy szerzői jogi védelemben vagy iparjogvédelmi oltalomban, továbbá a polgári jog eszközrendszere alapján üzleti titokként vagy know-how-ként jogi védelemben részesüljön. Amennyiben az ötlet egyéni, eredeti jelleggel rendelkezik, különösen zenei, irodalmi, tudományos, egyéb művészeti vagy szoftveralkotásban megvalósul, úgy a szerzői jogi védelem automatikusan, mégpedig a mű létrejöttével keletkezik. A jogi védelem nem feltétele a bejelentés vagy a nyilvántartásba vétel. Ugyanakkor a személy, mint alkotó tevékenységet végző, a társadalmi fejlődést elősegítő ember jogos igénye, hogy az általa alkotott mű a kívánságának megfelelő oltalmat kapjon. Az átlagot meghaladó szellemi teljesítmény végtermékét, tekintettel arra, hogy az jelentős mértékben újító, magas színvonalú, új megoldásokat előállító, kreatív, ezért a munkát és annak gyümölcsét, az alkotást megillető érdemmel honorálni kell. Napjaink jogi védelmi oltalma a szerzői védelmi lehetőség. A szellemi tulajdon jogterületeinek jogviszonyait kezdetben kiadói, majd alkotáscentrikus módon próbálták szabályozni. Ma már a szellemi alkotások értékesítési monopóliumát is védelmezik.[469] Napjaink jogszabályrendszere szerint szerzői jog azt illeti, aki a művet

[468] Szellemi Tulajdon Nemzeti Hivatala, https://www.sztnh.gov.hu/hu/mit-jelent/mit-jelent-a-szellemi-tulajdon, letöltés: 2019. június 1.

[469] Horváth Attila: A szellemi alkotások jogának története, a szerzői jogi védelem kialakulása, a jogalkotás kezdetei Magyarországon, Iparjogvédelmi és Szerzői Jogi Szemle, 11. (121.) évfolyam 4. szám, Budapest, 2016.

megalkotta, vagyis a szerzőt, és csak a nyilvánosságra hozott művek használhatók fel szabadon. A magyar jogrendben a szellemi alkotás a személyiség elválaszthatatlan részét képezi. A szellemi alkotásokkal kapcsolatos jogviszonyokban a jogi védelem alapja nem csupán az ember, valamint csak azt a személyt illeti ez a fajta védelem, aki a szellemi alkotást létrehozta. Továbbá jogi személy nem képes alkotói tevékenységre, mivel az alkotói tevékenység kizárólag emberi munka lehet, így ennek eredménye, a szellemi alkotás kizárólag csak az alkotó személyét illeti meg, tehát jogi személynek szellemi alkotáshoz fűződő személyiségi joga nincs. Ugyanakkor jogi személy megszerezheti a szellemi alkotás hasznosítására, rendelkezésére vonatkozó jogokat, de az alkotással kapcsolatos személyiségi jog ebben az esetben is az alkotó személyét illeti.[470]

A szellemi tulajdon, a szerzői jog kialakulásának mozzanatai

A szellemi alkotások jogának történeti áttekintésével megállapítható, hogy az írás és a nyomdai technikák tömeges elterjedésével közel egy időben megjelent annak védelmi igénye is. John Locke eszméje nagy utat tett meg a mai szabályozási rendszerig, és tagadhatatlan, hogy filozófiáját a mai napig figyelembe vesszük nemcsak itthon, de az Európai Unióban is. A felvilágosodás és az elmúlt évszázad közigazgatás tudománya, valamint az információelméletek megjelenésének és tudománnyá való fejlődésének időszaka oly mértékű állam-, természet- és technikai tudományi, ipari majd társadalmi változást eredményezett, amely nemcsak befolyásolta, de nagymértékben meghatározta és az elkövetkezendőkben meg fogja határozni társadalmunk jövőjét.

A szellemi alkotások jogvédelme, jelentősége és kialakulása

A szerzői jog területének viszonyait korábban kiadói oldalról való megközelítéssel, majd alkotáscentrikus módszer alapján próbálták meg szabályozni. A szellemi alkotások védelme napjainkban elsősorban két fő területre vonatkozik:

- a szerzői jogra, amely főleg a tudományos, a művészet és az irodalom területén létrejött alkotások védelmére hivatott. A szerzői jog általános jellegű védelem, ahol az oltalom a szerzői mű megalkotásával keletkezik. A legfőbb kritériuma a mű egyéni és eredeti jellege.

[470] Nemzeti Adatvédelmi és Információszabadság Hatóság, https://naih.hu/files/NAIH-jubileumi-szemelvenyek-az-informacios-jogok.pdf, letöltés: 2021. április 25.

„*Ezzel szellemi alkotások jogának magyar rendszere élesen elválasztja a személyt és a tulajdont, a szellemi alkotás nem tekinthető szellemi tulajdonnak, mert az azt megalkotó személy (pl.: szerző, szabadalmas, véd-jegyjogosult stb.) személyhez fűződő jogai forgalomképtelenségének következtében a szellemi alkotás tulajdonképpen a személyiség elválaszthatatlan részévé válik.*”

- az iparvédelmi jogra, amely összetettebb és speciálisabb, mint az előző meghatározás, mivel nem művészi, esztétikai megközelítést igénylő alkotások védelmét látja el, hanem a tudományos-műszaki jellegű alkotások védelmét szabályozza. Ezen jogviszonyok tekintetében az alkotáshoz kötődés kevésbé szoros, inkább objektív értékelést igényel. Az iparvédelmi jog gyakorlatorientált, gazdasági-vagyoni és tulajdonjogi jogviszonyok védelmére koncentrál. Az iparjogvédelem emellett átfogja a vállalat- és árujelzőkhöz fűződő érdekek oltalmát biztosító szabályokat.[471] [472]

A szerzői jog a szerzőnek vagy jogutódjának kizárólagos joga valamely irodalmi vagy művészeti alkotás körébe eső szellemi termék felett, amely általában írásjellel, képes ábrázolással, szóval vagy zenével kifejezett műnek tekinthető. Ilyen különösen az irodalmi mű, a zenei mű, a filmalkotás, a szobor, a festmény, a fénykép, a számítógépes programok, az építészeti terv, vagy térkép. A szerzői jogi védelem kizárólagos jellegű, mivel csak a jogosult és a jogosult által meghatározott személy (szerző, szerzőtársak, a szerző jogutódja) által megszerezhető, tehát mindenki más arra kötelezhető, hogy ezeket a jogokat tiszteletben tartsa, és tartózkodjon a jogosultságok megzavarásától. Visszatekintéssel megállapítható, hogy a szerzői tulajdon az ókorban, valamint még a középkorban is fogalmi képtelenségnek tűnt, hiszen a dologi, jogi testet öltött dolgokra irányult, a tulajdon joga és a tulajdon használatából eredő gyümölcs, mint szellemi termék és annak felhasználásra irányuló jogintézmény csak kezdetleges állapotban, illetve kialakulóban volt. A szerzői jog története, a műfelhasználások története a nyomtatás, a nyomdák és a kiadók megjelenésével azonban váratlan fordulatot vett.[473] A nyomdagépet 1476-ban Angliában honosította meg William Caxton, ám a fejlődés folytatására csaknem egy évszázadot kellett várni. 1557-ben I. Mária királynő egyetlen céhnek, a Könyviparosok Céhének (Stationers' Company) adományozott ellenőrzést a nyomtatások és könyv- illetve kiadások eladására. Az első királyi nyomtatási privilégium 1518-ból származik. A bejegyzésekben 1580 körül jelent meg legelőször a „*right to copy*" kifejezés, tehát a többszörözéshez való jog, amely a nyomtatási jognál tágabb jogosultságot jelent. A *stationers'*

[471] Szellemi Tulajdon Nemzeti Hivatala, https://www.sztnh.gov.hu/hu/szellemi-alkotas, letöltés: 2018. január 30.

[472] Horváth Attila, A szellemi alkotások jogának története, a szerzői jogi védelem kialakulása, a jogalkotás kezdetei Magyarországon, Iparjogvédelmi és Szerzői Jogi Szemle, 11. (121.) évfolyam 4. szám, Budapest, 2016.

[473] Fülöp Géza, Olvasók, könyvek, könyvtárak. A kezdetektől 1848-49-ig. I. kötet. A könyvnyomtatás feltalálása, Gutenberg. Magyar Médiapedagógiai Műhely, Budapest, 1993

„*A 15. század közepe új korszak kezdete a könyvkultúra, s általában az emberi művelődés történetében. Gutenberg találmányával – ennek lényege a betűk sorozatgyártásának, azaz egyforma betűk sokszorosításának a lehetősége, majd az e betűkből készített szedésről a sajtó felhasználásával történő több (szükség esetén több száz, sőt több ezer) azonos példány készítése – a kézzel írott könyv (a kódex) mellett megjelenik a nyomtatott könyv. Ez fokozatosan visszaszorítja a kézzel írott könyvet, s az írásos gondolatközlésben szinte egyeduralkodóvá válik.*"

copyright tehát céhkizárólagosságon alapuló intézmény, a későbbi, a szerző javára szóló törvényes copyright előfutára.[474] A nyomtatás feltalálásával megjelent az első felhasználási jogintézmény, a szerződési forma, azaz a kiadói szerződés is. Az újabb és újabb, fejlettebb technikai találmányok elterjedésével időközben könnyűvé és olcsóvá vált könyvnyomtatás, ami felkeltette a kalózkodók érdeklődését is. Említésre méltó Luther Márton (1483–1546) története is. Meglepő, hogy már az ő idejében is előfordultak kiadói jogosultság körében keletkező különböző visszaélések és perek. Luther Márton, aki korának egyik legolvasottabb írója volt, joggal háborodott fel műveinek általa nem megengedett sokszorosítása és terjesztése miatt.[475] Bár abban az időben még nem szabályozták, de minden befolyását latba vetette az ilyen és hasonló szerzői visszaélések, jogbitorlások ellen. A szellemi alkotások jogvédelmének kialakulására elsősorban Thomas Hobbes (1588–1679), John Locke (1632–1704), Samuel von Pufendorf (1632–1694) tulajdonra építő, majd Immanuel Kant (1724–1804), akit a szellemi alkotások atyának tartanak, személyközéppontú gondolatai hatottak. A nyomdagépek számának növekedésével Angliában, a király felségjogát gyakorolva, egyre szigorúbb módon szabályozta a könyvkereskedelmet, egyúttal védelmezve a kiadókat a kalózoktól. Az Engedélyezési Törvény (Licensing Act of 1662) a nyomtatási tartalomra vonatkozó első rendelet. Az engedélyezett könyvek hiteles nyilvántartásának megalapítása azzal a követelménnyel valósult meg, hogy letétbe kellett helyezni az engedélyezett könyv egy példányát. A letéteket a Stationers' Company kezelte.

A szellemi tulajdon átértékelése, a szerzői jog megjelenése

A magántulajdon a nyugati típusú társadalmi berendezkedések egyik legalapvetőbb intézménye. Napjainkban már a tulajdonjog elismerése a nyugati demokráciákban általánosan elfogadott jogintézmény. Az erkölcsi alapja a többség által törvényesített, azonban a világon nem minden demokrácia óvja ugyanakkora erőfeszítésekkel a tulajdont. A felvilágosodás korszakában átértékelődött a tulajdon fogalma. A feudalizmus korában a tulajdon, így a földtulajdon leegyszerűsítve a nemes (földesúr) illetve az egyház kezében volt, minden, a hasznosításából származó gyümölccsel együtt. John Locke tézise szerint a földi javak Istentől

[474] Bernárd Aurél, Tímár István, A szerzői jog kézikönyve. Közgazdasági és Jogi Kiadó, Budapest, 1973.

„*A megszerzett kizárólagosság a céhtagot haláláig illette. Ezután ismét a Stationers' Company rendelkezett a művel, amíg a kizárólagosságot a másik folyamodó céhtagra nem ruházta*."

[475] Horváth Attila, A szellemi alkotásokjogának története, a szerzői jogi védelem kialakulása, a jogalkotás kezdetei Magyarországon, Iparjogvédelmi és Szerzői Jogi Szemle, 11. (121.) évfolyam 4. szám, Budapest, 2016.

„*Ugyan mi az már édes nyomdász uraim, hogy egymást oly nyilvánosan raboljátok és lopjátok és egymást megrontjátok.*"

származnak, amelyek az emberi közösséget együttesen illetik meg. Ebben a természeti állapotban azonban ezek a javak nem használhatók és nem is élvezhetők, azokat művelni vagy hasznosítani kell ahhoz, hogy gyümölcsözzön. Szükséges, hogy az egyének a természeti javakat saját magántulajdonuk alá hajtsák, megműveljék, mégpedig úgy, hogy a saját munkájuk hozzáadásával értékkel ruházzák fel azokat. Locke véleménye szerint természeti állapotban a természeti javak bőségesen rendelkezésre állnak ahhoz, így mindenki saját maga számára a szükséges mennyiséget elő tudja állítani anélkül, hogy mást ezzel sértene. A tulajdon és a társadalmi igazságtalanság váltotta ki a tulajdon fogalmának átértékelését. John Locke nézete szerint a tulajdon és a társadalmi igazságtalanság összefonódott a feudalizmusban. Az önkény vagy a jogtalanság elsősorban a tulajdonjogok eltiprásában nyilvánult meg. Véleménye szerint az élethez való jog, a szabadságjog, a dolgok feletti uralom, így a földtulajdon is beletartozik a tulajdon fogalmába. De nemcsak a fogalmat vizsgálta, hanem a környezetét is, a „miért" van szükség egy adott tulajdonra a társadalomban és a „hogyan" keletkezett, illetve vezethető le annak jogintézménye.[476] [477] A földtulajdon példáját használva nemcsak saját érvelésével, de bibliai idézetekkel is próbálta igazolni nézeteit (*az Isten nemcsak megalkotta, de fiainak adományozta a földet*). Írásában nemcsak a fizikai alakot öltött, testi tárgyakra érti a fennálló tulajdont, hanem az élethez és a szabadsághoz fűződő emberi jogokat is ide gondolja. Tehát már megjelenik a tulajdon kiterjesztett tartalma, fogalma is. Az emberi munka pedig létrehoz egy produktumot, így a munkát végző személy javára tulajdon keletkezik. A befektetett munkaerő tulajdonosát illeti az eredmény gyümölcse is. A munkaerő itt már nem fizikai formát ölt, és annak gyümölcse sem feltétlenül ölt alakot, esetlegesen kézzel meg nem fogható, szellemi termék. Ennek az akkor még bonyolult összefüggésnek köszönhetjük, hogy az angol jogrendszer alkalmazhatta a tézist és elindulhatott a szellemi tulajdon és a szerzői tulajdon jogintézményének fejlődése és szabályozása. A kor eszméi nemcsak a tulajdon fogalmát szélesítették, hanem már a szabályozási rendszerben is változásokat hozott. Anglia és az angolszász közösség első modern szerzői jogi törvénye a Statute of Anne (Anna Királynő Törvénye, 1709). Két új jogintézményt deklarált, a szerző szerzői jogának tulajdonosát,

[476] John Locke, Two Treatises of Government (Két értekezés a polgári kormányzatról) 1689.

[477] Jakab Éva, Szerzők, kiadók, kalózok, a szellemi alkotások védelmének kialakulása Európában, Budapest Akadémiai Kiadó, 2012.

„*A tulajdon célját és legitimitását tehát a természeti erőforrások optimális kihasználásában látja." „Az optimális használat, az uralom alá hajtás csak a kizárólagos tulajdon révén válik lehetségessé*."

valamint a kiadott művek védelmi ideje határozott voltának elvét.[478] A törvény előírta, hogy az adott könyv megadott számú (kilenc) másolatát letétbe kell helyezni az ország meghatározott helyein, könyvtáraiban. Legfontosabb vívmánya, hogy megadta a szerzők számára a műveik feletti felügyelet jogát egy 14 éves, határozott időtartamra, amelyet újabb 14 évre meg lehetett újítani. Az ezt követő szerzői jogi törvények megalapozták a szerzői jogot más művek tekintetében is. A törvény megpróbálta megtörni a könyvkiadók-kereskedők egyeduralmát a *stationers' copyright* idejének 21 évre való korlátozásával – ez radikális változás volt a könyvkiadók számára, akik eddig örökös szerzői jogot élveztek. A Stationers' Company ezt nem hagyhatta annyiban, és az íróknak sem tetszett a határozott tartamú védelmi idő, hisz annak lejárta után már nem illette őket semmiféle jog (mivel a mű közkinccsé vált). Ily módon megindult a harc az örökös többszörözési jog, vagyis az időhatár nélküli copyright elismeréséért. A szerzői jog tulajdonjogi elmélete kompromisszumot adhatott a szerzői alkotás és az ebből származó tulajdon vitás eseteiben is, ami érintette a rendelkezési jogot, a kézirat elidegenítése után is a szerző rendelkezhet felőle, mindaddig, amíg a tulajdonjogát másra át nem ruházta. A tulajdon ellenérték fejében megvásárlási lehetőséget is biztosított. A szerzői jog történetében jelentős szereppel bír az a tény, hogy John Locke rámutatott a munka szerepére, mint a tulajdonjog forrására, ugyanakkor W. Warburton mondta ki végül a megfelelő kifejezést 1747-ben, szerzői tulajdon („*literary property*"). 1747-ben W. Warburton, Pope irodalmi hagyatékának gondozója, a Parlament egyik tagjához az irodalmi tulajdonról („literary propriety") névtelenül írt nyílt levelében tovább fejlesztette John Locke elméletét, és kiterjesztette azt, a nem dologi, tehát szellemi termékeken való tulajdonszerzés eseteire[479]. Rámutatott arra, hogy a könyv nem azonos a benne közölt írásművel, amelyet annak szerzője közre ad. A megalkotásával saját tulajdont szerzett, amit jogként kell védeni, és amit csak a szerző saját kizárólagos hasznára lehet többszörözni. Hasonlóan kimutatta a találmánytulajdoni különállását is az azt megvalósító szerkezettől. Az utóbbi megvalósításában a mechanikai kivitelezőnek a könyvnyomtatóhoz képest nagyobb szerepét ismerte fel, aminek következtében véleménye szerint, a feltalálónak nincs tökéletes tulajdonjoga a találmányán. Hasonló meggondolások alapján fejtette ki álláspontját Fichte 1793-ban, amely szerint valamely könyvben közölt elgondolások közkinccsé válhatnak mindenki számára, ugyanakkor a

[478] Part Krisztina Katalin, A szerzői jogi szabályozás kialakulása Angliában, Németországban és az Egyesült Államokban, Iparjogvédelmi és Szerzői Jogi Szemle, 1. (111.) évfolyam 4. szám, Budapest, 2006.

[479] A letter from an author to a member of Parliament; concerning literary Propriety, London, Warburton's Letter from an Author, London (1747), University of Birmingham Library: R. Hurd, ed., The Works of the Right Reverend William Warburton, 12 vols. (London: Cadell & Davies, 1811) Vol.12, 405-416,

kifejezések felett a szerzőnek elidegeníthetetlen tulajdonjoga van, míg a könyv példányai a kiadó elidegeníthető tulajdonát képezik.[480] [481] John Locke tulajdonelmélete és a szellemi javak létrejötte nemcsak véletlenül előálló tézisek sorozata. Az írás és olvasástudók számának növekedésével, a kéziratot kiadók általi kezeléssel, a nyomdák és nyilvántartások, majd könyvtárak elterjedésével az adott korban már nemcsak egy-egy eredeti szerzői példányt, hanem példányok sorozatát lelhetjük fel. A szerző védi a művét, illetve a kézirat eredetiségét, a személyéhez való kötöttséget és a megjelenésének darabszámát, ezzel szemben a nyomda a példányok megfelelő előállítási módját és példányszámát, a kiadó pedig a példányok megjelenését és kereskedését, az ebből származó bevételét. Jogos elvárás, hogy mindegyik érdek és eredmény, azaz a gyümölcs, amely mögött befektetett munka található, megfelelő védelmet kapjon. A legtöbb esetben John Locke tézise helytálló is. A természetjogi elmélet esetében, az ember a természetes állapotban lévő javakat dolgozza fel és teszi saját tulajdonává, ez pedig a természetjogból fakadóvá teszi a tulajdont.[482] A természetjogi alapon nyugvó megközelítés alapján a szellemi tulajdon nem volt eltérő a hagyományos testi tulajdontól, sőt, egyes gondolkodók szerint az ember saját ötletei képezik a legszentebb tulajdonát, szemben a fizikai világban jelenlévő tulajdonnal.

A szellemi alkotások védelme és a szerzői jog szabályai napjainkban

Napjainkban jogszabályok által is védik, támogatják a szellemi termékeket. Egy információs rendszer adatbázisa „*önmagában szerzői jogvédelmet nem élvező tényközléseket és önálló szerzői jogi védelmet is élvező*" adatokat tartalmazhat.[483] Az, hogy az adott adatbázis melyik

---

[480] Fichte, Beweis der Unrechtmäßigkeit des Büchernachdrucks. Berliner Monatsschrift, Vol. 21., 1793

[481] Boytha György, A szellemi alkotások joga és az új Ptk., Polgári Jogi Kodifikáció, 2000/2., 46-56. o., Budapest

[482] Keserű Barna Arnold, John Locke tulajdonelmélete a szellemi tulajdonjogok nézőpontjából, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar, 2016

[483] A szerzői jog gyakorlati kérdései, Válogatás a Szerzői Jogi Szakértő Testület szak véleményeiből (2010 –2013) fennállásának 130. év fordulója alkalmából, Szellemi Tulajdon Nemzeti Hivatala, Szerkesztő: Legeza Dénes, Felelős kiadó: dr. Bendzsel Miklós, 2014.

„*Ha tehát feltesszük az előző pont szerint, hogy a megkeresésben leírt adatbázisok megfelelnek az adatbázis Szjt. 60/A. § szerinti fogalmának, és az M. adatbázis-előállítónak minősül, azt kell megvizsgálni, hogy fennállnak-e a szóban forgó adatbázisokra a kapcsolódó jogi védelem feltételei.*"

„*Az Szjt. 84/A. §-ának (5) bekezdése szerint az adatbázis-előállító akkor rendelkezik az ún. sui generis jogokkal, ha az adatbázis tartalmának megszerzése, ellenőrzése vagy megjelenítése jelentős ráfordítást igényelt.*"

„*az a körülmény, hogy valamely adatbázis létrehozása olyan főtevékenység gyakorlásához kapcsolódik, amelynek keretében az adatbázist létrehozó személy egyben ezen adatbázist alkotó tartalmi elemek létrehozója is, mint olyan nem zárja ki azt, hogy ez a személy igényelhesse a sui generis jog által biztosított védelmet, feltéve, hogy bizonyítja, hogy e tartalmi elemeknek ... megszerzése, ellenőrzése, illetve előállítása mennyiségi vagy minőségi szempontból jelentős, és az e tartalmi elemek létrehozására felhasznált pénzeszközöktől független ... ráfordítást igényelt.*"

kategóriába tartozik, csak egyedi vizsgálat alapján lehet meghatározni. Amennyiben egy adatbázis „*tartalmi elemek létrehozatalára eszközölt ráfordítások levonása után is jelentős ráfordítás eredményeként jött létre, így jogosult a sui generis oltalomra*". A szellemi alkotásra és a szerzői jogra vonatkozó szabályokon és előírásokon kívül, elektronikus világunkban a közigazgatási adatbázisok összekapcsolásának kötelezettségét, a szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény[484] is szabályozza. Ez által biztosíthatják nemcsak az informatikai rendszerekben tárolt információk védelmét, de az informatikai rendszer által elérhetővé vált szellemi termékek, művek, alkotások és alkalmazások sértetlenségét, biztonságát és rendelkezésre állását.[485] Az adatbázisban tárolt információkat, úgynevezett anonimizálás vagy álnevesítés módszerének alkalmazásával, további védelemmel lehet ellátni annak érdekében, hogy az adatbázisból kinyert, például személyre vonatkozó adatokat ne lehessen azonosítani, illetve egy adott személyhez visszavezetni. Az említett módszereket különösen anonim kérdőív gyakorlati megvalósításához[486], statisztikai kimutatáshoz, vezetői információs rendszerek forrás adatainak előállításához (Adattár Alapú Vezetői Információs Rendszer - AVIR) lehet használni, de egy irodalmi műre, kivonatok elkészítéséhez, adattovábbítási eljáráshoz vagy nyilvánosságra hozatali kötelezettség teljesítéséhez is jól alkalmazható.[487] A Nemzeti Adatvédelmi és Információszabadság Hatóság a gyakorlati útmutató hét tanácsával segíti az adatkezelők, a személyes adatok védelmére vonatkozó tevékenységét. A módszerek alkalmazásával

[484] 2007. évi CI. törvény, a döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról

[485] Szellemi alkotásra és a szerzői jogra vonatkozó legfontosabb szabályok, előírások:

1999. évi LXXVI. törvény a szerzői jogról

1997. évi XI. törvény a védjegyek és a földrajzi árujelzők oltalmáról

1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról

1995. évi XXXIII. törvény a találmányok szabadalmi oltalmáról

2001. évi XLVIII. törvény a formatervezési minták oltalmáról

1991. évi XXXVIII. törvény a használati minták oltalmáról

2014. évi LXXVI. törvény a tudományos kutatásról, fejlesztésről és innovációról

1991. évi XXXIX. törvény a mikroelektronikai félvezető termékek topográfiájának oltalmáról

2016. évi XCIII. törvény a szerzői jogok és a szerzői joghoz kapcsolódó jogok közös kezeléséről

138/2014. (IV. 30.) Korm. rendelet az árva mű felhasználásának részletes szabályairól

[486] Nemzeti Adatvédelmi és Információszabadság Hatóság, A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), közleménye az Erzsébet-táborokban a táborozó gyermekek részére készített, „Véleményed kincs!" című kérdőívhez kapcsolódó adatkezelést illetően, 2020.

[487] NAIH-1938-2/2013/T, Gyakorlati útmutató védett adatot nem tartalmazó kivonat készítéséhez, NAIH, 2014., https://naih.hu/files/2014_02_03_anonimizalas_gyak_utm.pdf, letöltés: 2022. január 14.

csökkenthető az adatkezelés kockázata, elősegíthető a szükséges, GDPR és Infotv. előírások szerinti szervezési és technikai intézkedések teljesítése.